

①2 DEMANDE DE BREVET D'INVENTION

A1

②2 Date de dépôt : 18.12.15.

③0 Priorité :

④3 Date de mise à la disposition du public de la
demande : 23.06.17 Bulletin 17/25.

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

⑥0 Références à d'autres documents nationaux
apparentés :

○ Demande(s) d'extension :

⑦1 Demandeur(s) : OBERTHUR TECHNOLOGIES
Société anonyme — FR.

⑦2 Inventeur(s) : DEPRUN JEAN-FRANCOIS, SEGA-
LOU DAVID et ALZAI ERIC.

⑦3 Titulaire(s) : OBERTHUR TECHNOLOGIES Société
anonyme.

⑦4 Mandataire(s) : SANTARELLI.

⑤4 PROCÉDE DE GESTION DES CONNEXIONS ENTRE UN ÉLÉMENT SÉCURISÉ ET UN SERVEUR.

⑤7 Un procédé de gestion des connexions entre un élé-
ment sécurisé et un serveur (30) d'un réseau de communi-
cation, ledit élément sécurisé (20) étant incorporé dans un
dispositif hôte (10).

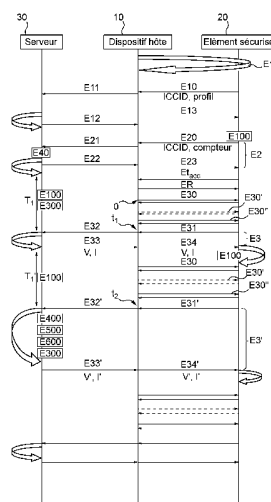
Le procédé comporte les étapes suivantes :

- détermination (E300) d'une période de temps théo-
rique entre deux instants de connexion consécutifs,
- détermination (E400) d'une période de temps réelle
entre deux instants de connexion consécutifs entre ledit élé-
ment sécurisé et ledit serveur,

- comparaison (E500) de ladite période de temps théo-
rique déterminée avec la période de temps réelle détermi-
née, et

si la période de temps théorique déterminée est diffé-
rente de la période de temps réelle déterminée :

- détermination d'une nouvelle période de temps théo-
rique.



5 La présente invention concerne un procédé de gestion des connexions entre un élément sécurisé et un serveur d'un réseau de communication.

Elle concerne en particulier un procédé de gestion des connexions dites « *Over-The-Air* » ou connexions OTA.

10 Un élément sécurisé, tel qu'une carte à puce par exemple, est incorporé dans un dispositif hôte. Le dispositif hôte est, par exemple, un téléphone portable, une tablette numérique ou tout autre équipement électronique tel qu'un compteur électrique, un véhicule, une machine à café, etc.

15 Un élément sécurisé peut être par exemple une carte de type UICC (pour « *Universal Integrated Circuit Card* ») visée dans la norme ETSI TS 102 221, et regroupe les cartes à puce classiques, type carte SIM (ou USIM – pour « *Universal Subscriber Identity Module* »), mais également des jetons (*token*) sécurisés, ou par exemple une carte de type eUICC (pour « *embedded*
20 *Universal Integrated Circuit Card* ») et visée dans la norme ETSI TS 103 383.

L'élément sécurisé peut être aussi un élément sécurisé embarqué (ou eSE) connu en terminologie anglo-saxonne comme « *embedded Secure Element* ».

25 Le serveur auquel l'ensemble d'éléments sécurisés se connecte fait partie d'un réseau de communication comportant un ensemble d'équipements d'un opérateur permettant la connexion et la connectivité de ses abonnés.

Lorsqu'une connexion entre un élément sécurisé et le serveur est établie, des données concernant l'élément sécurisé ou le dispositif hôte sont mises à jour.

30 Par exemple des données stockées ou des applications installées dans l'élément sécurisé ou dans le dispositif hôte sont mises à jour avec des

nouvelles données, des nouvelles fonctionnalités ou des nouveaux services proposés par l'opérateur.

La connexion entre un élément sécurisé et un serveur peut être mise en œuvre à l'initiative du serveur ou de l'élément sécurisé. Lorsque la connexion est mise en œuvre à l'initiative du serveur (connu comme « *mode Push* »), le serveur envoie un message au dispositif hôte, par exemple de type SMS, l'élément sécurisé initiant alors une connexion OTA avec le serveur à réception du SMS dans le dispositif de connexion. Lorsque la connexion est mise en œuvre à l'initiative de l'élément sécurisé (connu comme « *mode Pull* »), l'élément sécurisé initie la connexion avec le serveur à travers le dispositif hôte.

Les nouvelles générations de réseaux de communication mobiles, comme par exemple les réseaux de communication LTE (« *Long Term Evolution* », connus comme « *réseaux 4G* ») n'utilisent pas nécessairement les SMS et par conséquent ne peuvent pas mettre en œuvre le mode de connexion dit « *mode Push* ». Dans de tels réseaux de communication, les connexions entre les éléments sécurisés et le serveur sont établies à l'initiative des éléments sécurisés.

Des instants de connexion ainsi qu'une période de temps écoulé entre deux instants de connexion consécutifs sont associés à chaque élément sécurisé.

Afin d'éviter la saturation du serveur, les instants de connexion auxquelles les connexions, par exemple des connexions OTA, qui sont établies entre les éléments sécurisés et le serveur sont étalés dans le temps. Pour cela, les instants de connexion et la période de temps entre deux instants de connexion consécutifs associés aux éléments sécurisés doivent être respectivement différents.

La période de temps entre deux instants de connexion consécutifs peut être déterminée par l'élément sécurisé et/ou par le serveur et est fonction d'un intervalle d'accès (nommé « *polling interval* » en terminologie anglo-saxonne), l'intervalle d'accès représentant l'intervalle de temps entre deux accès consécutifs du dispositif hôte à l'élément sécurisé. Cette période de temps déterminée est une période de temps théorique.

En particulier, la période de temps entre deux instants de connexion consécutifs correspond à un nombre d'intervalles d'accès.

L'intervalle d'accès est propre au dispositif hôte, mais l'élément sécurisé peut solliciter le dispositif hôte pour établir l'intervalle d'accès à une
5 valeur souhaitée.

Néanmoins, certains dispositifs hôte ne présentent pas de fonctionnalité leur permettant de modifier leur intervalle d'accès ou bien ne tiennent pas compte de la requête issue de l'élément sécurisé pour modifier cette valeur ou ne respectent pas la valeur demandée par l'élément sécurisé et
10 imposent la leur.

Ainsi, la période de temps entre deux instants de connexion consécutifs déterminée par l'élément sécurisé et/ou par le serveur, ou période de temps théorique, présente un écart par rapport à la période de temps réelle entre deux instants de connexion consécutifs.

La présente invention propose d'optimiser la gestion des connexions entre les éléments sécurisés et les serveurs d'un réseau de communication.
15

A cet effet, la présente invention propose selon un premier aspect, un procédé de gestion des connexions entre un élément sécurisé et un serveur
20 d'un réseau de communication, l'élément sécurisé étant incorporé dans un dispositif hôte, le procédé de gestion des connexions comportant les étapes suivantes :

- détermination d'une période de temps théorique entre deux instants de connexion consécutifs entre l'élément sécurisé et le serveur en
25 fonction d'un ensemble de paramètres et d'un intervalle d'accès théorique associé audit dispositif hôte,

- détermination d'une période de temps réelle entre deux instants de connexion consécutifs entre l'élément sécurisé et le serveur,

- comparaison de ladite période de temps théorique avec la période
30 de temps réelle déterminée, et

si la période de temps théorique déterminée est différente de la période de temps réelle déterminée :

- modification d'au moins un paramètre de l'ensemble des paramètres de sorte que la période de temps théorique présente une valeur proche de la période de temps réelle déterminée, et

- détermination d'une nouvelle période de temps théorique prenant
5 en compte ledit au moins un des paramètres modifié.

Ainsi, en modifiant la valeur d'au moins un paramètre, la période de temps théorique déterminée peut être modifiée de sorte qu'elle soit similaire ou tendre au plus près de la période de temps réelle entre des connexions consécutives entre l'élément sécurisé et le serveur.

- 10 Par conséquent, cette période de temps théorique peut être adaptée même lorsque le dispositif hôte ne présente pas la fonctionnalité lui permettant de modifier l'intervalle d'accès ou ne tient pas compte de la requête provenant de l'élément sécurisé pour modifier la valeur de l'intervalle d'accès.

- 15 Selon une caractéristique, le procédé comporte une étape de détermination de la valeur d'un paramètre n en utilisant ledit ensemble de paramètres.

- 20 Selon une caractéristique, la détermination de ladite période de temps théorique comporte une étape de multiplication de l'intervalle d'accès théorique par ladite valeur dudit paramètre n déterminée, le résultat étant ladite période de temps théorique.

Ainsi, la période de temps théorique est égale à l'intervalle d'accès théorique multiplié par la valeur du paramètre n déterminée, la valeur du paramètre n étant déterminée en fonction de l'ensemble de paramètres.

- 25 Selon une autre caractéristique, l'étape de détermination de la période de temps réelle comporte une étape de comptage, mise en œuvre par l'élément sécurisé, d'un nombre d'intervalles d'accès réels du dispositif hôte à l'élément sécurisé, la période de temps réelle étant équivalente au temps écoulé lors du comptage d'un nombre d'intervalles d'accès réels égal à la valeur du paramètre n déterminé.

- 30 Grâce à l'étape de comptage, l'élément sécurisé détermine de son côté, la période de temps réelle et par conséquent les instants de connexion au serveur. Cette étape de comptage met en œuvre un compteur pour compter un

nombre d'intervalles d'accès réels. Lorsque le nombre d'intervalles d'accès réels comptés ou la valeur du compteur est égale à la valeur du paramètre n , une période de temps réelle s'est écoulée et l'élément sécurisé établit une connexion avec le serveur.

5 Ainsi, les instants de connexion sont déterminés au moyen du comptage d'intervalles d'accès, en nombre équivalant à la valeur du paramètre n , la période de temps écoulée entre deux instants de connexion consécutifs étant représentée par l'intervalle d'accès répété un certain nombre de fois, le nombre de fois étant déterminé en fonction de l'ensemble des paramètres.

10 Selon une caractéristique, le procédé comporte une étape d'envoi, mise en œuvre par l'élément sécurisé, dans laquelle la dernière valeur du paramètre n atteinte à l'étape de comptage d'un nombre d'intervalles d'accès réels avant que le dispositif hôte ne soit éteint ou redémarré est envoyée au serveur, ladite étape d'envoi étant mise en œuvre lorsque ledit dispositif hôte,
15 initie une phase d'initialisation avec le serveur, la phase d'initialisation étant mise en œuvre après son allumage ou redémarrage du dispositif hôte.

 Ainsi, la détermination de la période de temps théorique tient compte de l'évolution de la valeur du paramètre n dans ses connexions précédentes.

 Selon des modes de réalisation différents, le serveur peut tenir
20 compte de la valeur du paramètre reçu à l'allumage du dispositif hôte ou l'ignorer.

 Selon une caractéristique, l'ensemble de paramètres comporte un paramètre d'identification unique, un premier paramètre et un second paramètre.

25 L'utilisation des premier et second paramètres dans la détermination de la période de temps entre deux instants de connexion consécutifs permet d'obtenir des valeurs différentes du paramètre n , et par conséquent des périodes de temps théoriques pour un même élément sécurisé.

 Les valeurs des premier et second paramètres sont stockées dans
30 l'élément sécurisé lors de sa fabrication et sont ensuite modifiées pendant l'utilisation de l'élément sécurisé.

Selon une caractéristique, après la phase d'allumage ou de redémarrage et la phase d'initialisation, le procédé comporte l'établissement d'une première connexion à un premier instant de temps ledit premier instant de connexion a une valeur comprise entre un premier instant de temps
5 prédéterminé et un second instant prédéterminé.

Ainsi, les premier et second paramètres sont déterminés de sorte que la valeur du paramètre n ait une valeur telle que le premier instant de connexion soit compris entre un instant de temps minimal et un instant de temps maximal.

10 En outre, le serveur connaît l'intervalle dans laquelle l'élément sécurisé doit se connecter.

Par conséquent, la sécurité dans les connexions entre l'élément sécurisé et le serveur est améliorée. Ceci est particulièrement avantageux pour la première connexion au serveur établie par l'élément sécurisé.

15 Selon une caractéristique, le procédé comporte une étape de détermination, mise en œuvre par le serveur, de l'intervalle d'accès réel associé au dispositif hôte à partir de la période de temps réelle et de la valeur du paramètre n déterminée.

Ainsi, une fois que l'élément sécurisé a établi deux connexions
20 consécutives au serveur, le serveur connaît la période de temps réelle et la valeur du paramètre n , et peut ainsi déterminer l'intervalle d'accès réel.

Selon un mode de réalisation, l'étape de modification est mise en œuvre par le serveur et le procédé comporte en outre une étape d'envoi, mise en œuvre par le serveur, dans laquelle ledit au moins un paramètre modifié est
25 envoyé audit élément sécurisé, ladite étape de détermination d'une nouvelle période de temps théorique étant mise en œuvre par ledit élément sécurisé en utilisant ledit au moins un paramètre modifié reçu.

Dans ce mode de réalisation, le serveur modifie au moins un paramètre de l'ensemble de paramètres et l'envoie à l'élément sécurisé. La
30 valeur du paramètre n est déterminée en fonction de l'ensemble de paramètres par l'élément sécurisé.

Selon un autre mode de réalisation, l'étape de modification et l'étape de détermination d'une nouvelle période de temps théorique sont mises en œuvre par ledit serveur, et le procédé comporte en outre une étape d'envoi, mise en œuvre par le serveur, dans laquelle ladite nouvelle période de temps
5 théorique déterminée est envoyée à l'élément sécurisé.

Ainsi, selon ce mode de réalisation, la période de temps théorique est déterminée par le serveur en fonction de l'ensemble de paramètres modifié. La période de temps théorique déterminée est ensuite envoyée à l'élément sécurisé, l'élément sécurisé prenant en compte cette nouvelle période
10 déterminée pour la prochaine connexion au serveur.

Selon une caractéristique, le procédé de gestion des connexions comporte la création d'une structure de données comportant des données relatives à un ensemble d'éléments sécurisés, lesdites données relatives audit ensemble d'éléments sécurisés étant pour chaque élément sécurisé de
15 l'ensemble, ladite période de temps théorique déterminée, ladite période de temps réelle déterminée, l'intervalle d'accès théorique déterminé, l'intervalle d'accès réel déterminé et le nombre d'intervalles d'accès comptés lors de l'étape de comptage.

Ainsi, les périodes de temps réel et théorique déterminées, les
20 intervalles d'accès théoriques et réels déterminés pour chaque élément sécurisé et le nombre d'intervalles d'accès comptés par chaque élément sécurisé sont stockées dans la structure de données. Cette structure de données recueille alors les dernières périodes de temps (réelles et théoriques) déterminées et les derniers intervalles d'accès (réels et théoriques) déterminés
25 pour chaque élément sécurisé de l'ensemble, ainsi que le nombre d'intervalles d'accès comptés avant que le dispositif hôte soit éteint ou redémarré.

La structure de données comprend également le numéro d'identifiant ou paramètre d'identification unique de l'élément sécurisé, le profil du dispositif hôte (« *terminal profile* » en terminologie anglo-saxonne), la valeur du compteur
30 d'intervalles d'accès et un premier instant de temps prédéterminé et un second instant de temps prédéterminé.

Selon une caractéristique, la structure de données est stockée dans le serveur, et est mise à jour lorsqu'une des données est déterminée ou reçue.

Ainsi, le serveur et l'élément sécurisé utilisent des valeurs des périodes de connexion et d'intervalle d'accès mis à jour.

5 L'invention concerne selon un deuxième aspect, un serveur d'un réseau de communication comportant des moyens de connexion avec un ensemble d'éléments sécurisés, chaque élément sécurisé étant incorporé dans un dispositif hôte, le serveur comportant pour chaque élément sécurisé :

- des moyens de détermination d'une période de temps théorique
10 entre deux instants de connexion consécutifs entre l'élément sécurisé et le serveur en fonction d'un ensemble de paramètres et d'un intervalle d'accès théorique associé au dispositif hôte,

- des moyens de détermination d'une période de temps réelle entre
deux instants de connexion consécutifs entre l'élément sécurisé et le serveur,

15 - des moyens de comparaison de la période de temps théorique déterminée avec la période de temps réelle déterminée,

- des moyens de modification d'au moins un paramètres de
l'ensemble des paramètres de sorte que la période de temps théorique présente une valeur proche de la période de temps réelle déterminée si la
20 période de temps théorique déterminée est différente de la période de temps réelle déterminée, et

- des moyens de détermination d'une nouvelle période de temps théorique prenant en compte au moins un des paramètres modifié.

25 Selon une caractéristique, le serveur comporte en outre des moyens de détermination de la valeur d'un paramètre n en utilisant l'ensemble de paramètres.

Selon une caractéristique, le serveur comporte des moyens de détermination de la période de temps théorique comportant des moyens de multiplication de l'intervalle d'accès théorique par la valeur du paramètre n
30 déterminée, le résultat de la mise en œuvre des moyens de multiplication étant la période de temps théorique.

Selon une caractéristique, le serveur comporte des moyens de réception de la dernière valeur du paramètre n atteinte par les moyens de comptage d'un nombre d'intervalles d'accès réels dans l'élément sécurisé, avant que le dispositif hôte ne soit éteint ou redémarré, la dernière valeur dudit paramètre n étant envoyée par l'élément sécurisé lorsque le dispositif hôte initie une phase d'initialisation avec le serveur, la phase d'initialisation étant mise en œuvre après l'allumage ou le redémarrage dudit dispositif hôte.

Selon une autre caractéristique, le serveur comporte des moyens de détermination du premier paramètre et du second paramètre de sorte que le premier instant de connexion a une valeur comprise entre un premier instant de temps prédéterminé et un second instant prédéterminé.

Selon une autre caractéristique, le serveur comporte des moyens de détermination de l'intervalle d'accès réel associés au dispositif hôte à partir de la période de temps réelle et de la valeur du paramètre n déterminée.

Selon une caractéristique, le serveur comporte des moyens d'envoi configurés pour envoyer à l'élément sécurisé au moins un paramètre de l'ensemble de paramètres modifié.

Selon une autre caractéristique, les moyens d'envoi sont en outre configurés pour envoyer audit élément sécurisé ladite nouvelle période de temps théorique déterminée.

Selon une caractéristique, le serveur comporte des moyens de création d'une structure de données comportant des données relatives à un ensemble d'éléments sécurisés, les données relatives à l'ensemble d'éléments sécurisés étant pour chaque élément sécurisé de l'ensemble, la période de temps théorique déterminée, la période de temps réelle déterminée, l'intervalle d'accès théorique, l'intervalle d'accès réel déterminé et le nombre d'intervalles d'accès comptés lors de l'étape de comptage.

Selon une autre caractéristique, le serveur comporte des moyens de stockage de ladite structure de données et des moyens de mise à jour de ladite structure de données lorsqu'au moins une des données dans la structure de données est déterminée.

Par ailleurs, le serveur comporte en outre des moyens de détermination, pour chaque élément sécurisé, des instants de connexion au serveur en fonction d'un paramètre d'identification unique associé à l'élément sécurisé.

5 Selon une caractéristique, le serveur comporte des moyens de modification configurés pour modifier la valeur dudit premier paramètre et dudit second paramètre à des instants prédéfinis.

 Ainsi, les instants de connexion déterminés peuvent être modifiés pour un même élément sécurisé. Par exemple, comme indiqué ci-dessus, les
10 instants de connexion peuvent ainsi être modifiés après chaque connexion entre l'élément sécurisé et le serveur, et peuvent être difficilement déduits par des dispositifs tiers.

 La sécurité dans les connexions entre les éléments sécurisés de l'ensemble et le serveur est, par conséquent, davantage améliorée.

15 La modification des premier et second paramètres par le serveur est particulièrement avantageuse dans le cas d'un dispositif hôte qui ne respecterait pas une demande, de la part et en provenance d'un élément sécurisé d'utiliser une valeur d'intervalle d'accès (« *Polling Interval value* ») transmise par une requête de demande de modification de l'intervalle d'accès,
20 bien connue de l'homme du métier par commande proactive « Poll Interval ». Dans ce cas, le serveur modifie les premier et second paramètres de sorte que les instants de connexion déterminés soient en adéquation avec les caractéristiques du dispositif hôte et avec les attentes du serveur.

 L'invention concerne selon un troisième aspect, un élément sécurisé
25 comprenant des moyens de gestion des connexions avec un serveur d'un réseau de communication, caractérisé en ce qu'il comporte en outre :

- des moyens de détermination de la valeur d'un paramètre n en utilisant un ensemble de paramètres, ledit ensemble de paramètres comportant un paramètre d'identification unique associé audit élément sécurisé, un premier
30 paramètre et un second paramètre,
- des moyens de détermination de la période de temps réelle entre deux instant de connexion consécutifs au serveur, et

- des moyens d'établissement d'une connexion avec le serveur à des instants de connexion.

Par exemple, l'élément sécurisé peut être un élément sécurisé de type UICC, un élément sécurisé de type UICC embarqué (eUICC) ou élément
5 sécurisé embarqué (eSE).

Selon une caractéristique, les moyens de détermination de la période de temps réelle comporte des moyens de comptage d'un nombre d'intervalles d'accès réelles du dispositif hôte à l'élément sécurisé, la période de temps réelle étant équivalente au temps écoulé lors du comptage d'un nombre
10 d'intervalles réelles d'accès égal à la valeur du paramètre n déterminé par les moyens de détermination.

L'invention concerne selon un quatrième aspect, un dispositif hôte comportant un élément sécurisé conforme à l'invention.

Dans un mode de réalisation, le dispositif hôte est un terminal mobile
15 de communication.

L'élément sécurisé, le serveur et le dispositif hôte présentent des caractéristiques et avantages analogues à ceux décrits précédemment en relation avec le procédé de gestion des connexions.

Dans un mode particulier de réalisation, les différentes étapes du procédé précité sont déterminées par des instructions de programmes d'ordinateurs.
20

En conséquence, l'invention vise aussi un programme d'ordinateur sur un support d'informations, ce programme étant susceptible d'être mis en œuvre par un microprocesseur, ce programme comprenant des instructions
25 adaptées à la mise en œuvre des étapes du procédé tel que mentionné ci-dessus.

Ce programme peut utiliser n'importe quel langage de programmation, et être sous la forme de code source, code objet, ou de code intermédiaire entre code source et code objet, tel que dans une forme
30 partiellement compilée, ou dans n'importe quelle autre forme souhaitable.

L'invention vise aussi un support d'informations lisible par un microprocesseur, et comprenant des instructions d'un programme d'ordinateur tel que mentionné ci-dessus.

5 Le support d'informations peut être n'importe quelle entité ou dispositif capable de stocker le programme. Par exemple, le support peut comprendre un moyen de stockage, tel qu'une ROM, par exemple une ROM de microcircuit, ou encore un moyen d'enregistrement magnétique, par exemple un disque dur, ou encore une mémoire flash.

10 D'autre part, le support d'informations peut être un support transmissible tel qu'un signal électrique ou optique, qui peut être acheminé via un câble électrique ou optique, par radio ou par d'autres moyens. Le programme selon l'invention peut être en particulier téléchargé sur une plateforme de stockage d'un réseau de type Internet.

15 Alternativement, le support d'informations peut être un circuit intégré dans lequel le programme est incorporé, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution du procédé en question.

Le support d'informations et le programme d'ordinateur précités présentent des caractéristiques et avantages analogues au procédé qu'ils mettent en œuvre.

20 D'autres particularités et avantages de l'invention apparaîtront encore dans la description ci-après.

Aux dessins annexés, donnés à titre d'exemples non limitatifs :

- la figure 1 représente schématiquement un contexte dans lequel un mode de réalisation de la présente invention est mis en œuvre ;

25 - la figure 2 représente schématiquement un dispositif hôte comprenant un élément sécurisé conforme à un mode de réalisation de l'invention ;

- la figure 3 représente un schéma dans lequel des connexions dans le temps sont représentées ; et

30 - la figure 4 représente schématiquement des étapes d'un procédé de gestion de connexion entre un élément sécurisé et un serveur selon un mode de réalisation de l'invention.

La Figure 1 représente un ensemble de dispositifs hôte 10, chacun des dispositifs hôte comportant un élément sécurisé 20.

Bien entendu, chaque dispositif hôte 10 peut comporter un nombre différent d'éléments sécurisés 20.

5 Les dispositifs hôte 10 sont par exemple des téléphones portables, des tablettes numériques ou tout autre équipement électronique tel qu'un compteur électronique, un véhicule, une machine à café, etc.

Cet ensemble de dispositifs hôte peut comporter différents types d'éléments sécurisés, c'est-à-dire il peut comporter par exemple un sous-ensemble de téléphones portables, un sous-ensemble de tablettes, ainsi que
10 d'autres sous-ensembles d'un autre équipement électronique.

L'élément sécurisé 20 est par exemple une carte à circuit intégré universelle (UICC) ou une carte à circuit intégré universelle et embarquée (eUICC) ou bien encore un élément sécurisé de type eSE.

15 Les éléments sécurisés 20 de l'ensemble peuvent communiquer avec un réseau de communication 300 comportant un ensemble d'équipements d'un opérateur permettant la connexion et la connectivité de ses abonnés.

En particulier, l'ensemble d'équipements de l'opérateur comporte un serveur 30 avec lequel communiquent les éléments sécurisés 20 de l'ensemble
20 et à partir duquel des données concernant les éléments sécurisés 20 ou les dispositifs hôtes 10 sont mises à jour.

La Figure 2 représente schématiquement un dispositif hôte 10 comprenant un élément sécurisé 20 conforme à un mode de réalisation de l'invention.

25 Le dispositif hôte 10 comprend un bus de communication 100 auquel sont reliées :

- une unité de traitement 11, nommée sur la figure CPU (pour « *Central Processing Unit* ») et pouvant comporter un ou plusieurs processeurs ;
- 30 - une mémoire non volatile 12, par exemple ROM (pour « *Read Only Memory* »), EEPROM (pour « *Electrically Erasable Read Only Memory* ») ou une mémoire Flash;

- une mémoire vive 13 ou RAM (pour « *Random Access Memory* ») ;
- une interface 14 d'entrée/sortie, nommée sur la figure I/O (pour « *Input/Output* »), par exemple un écran, un clavier, une souris ou un autre dispositif de pointage tel qu'un écran tactile ou une télécommande permettant à un utilisateur d'interagir avec le système via une interface graphique ; et
- une interface de communication 15, nommée COM sur la figure, adaptée à échanger des données par exemple avec un serveur via un réseau, ou une interface de lecture/écriture.

L'élément sécurisé 20 comprend un bus de communication 200 auquel sont reliées :

- une unité de traitement 21 ou microprocesseur, nommée sur la figure CPU (pour « *Central Processing Unit* ») ;
 - une mémoire non volatile 22, par exemple ROM (pour « *Read Only Memory* »), EEPROM (pour « *Electrically Erasable Read Only Memory* ») ou mémoire Flash;
 - une mémoire vive 23 ou RAM (pour « *Random Access Memory* ») ;
- et
- une interface de communication 24, nommée COM sur la figure, adaptée à échanger des données avec le processeur 11 du dispositif hôte 10.

La mémoire vive 23 comprend des registres adaptés à l'enregistrement des variables et paramètres créés et modifiés au cours de l'exécution d'un programme informatique comprenant des instructions pour la mise en œuvre d'un procédé selon l'invention. Les codes d'instructions du programme stocké en mémoire non-volatile 22 sont chargés en mémoire RAM 23 en vue d'être exécutés par l'unité de traitement CPU 21.

La mémoire non-volatile 22 est par exemple une mémoire réinscriptible de type EEPROM ou mémoire Flash pouvant constituer un support au sens de l'invention, c'est-à-dire pouvant comprendre un programme informatique comprenant des instructions pour la mise en œuvre des procédés selon l'invention.

La Figure 3 représente une ligne de temps dans laquelle des instants de connexion d'un élément sécurisé 20 à un serveur 30 sont représentés.

Cette figure illustre des instants de connexion $t_1, t_2, \dots, t_n$, en particulier un premier instant de connexion t_1 et un deuxième instant de connexion t_2 , les instants de connexion t_1, t_2 correspondant à deux connexions consécutives établies entre un élément sécurisé 20 de l'ensemble et le serveur 30.

5 Le temps écoulé entre les deux connexions consécutives ou deux instants de connexion t_1, t_2 consécutifs correspond à une période de temps réelle qui sera nommée dans le document période de connexion T .

Lorsque le dispositif hôte 10 est allumé et que sa phase d'allumage et d'initialisation est mise en œuvre, le dispositif hôte 10 accède périodiquement
10 à l'élément sécurisé 20. Par exemple, lors d'un accès, le dispositif hôte 10 envoie une commande (commande « STATUS ») à l'élément sécurisé 20. Ainsi, l'élément sécurisé 20 reçoit périodiquement la commande « STATUS » de la part du dispositif hôte 10.

Le temps écoulé entre l'envoi de deux commandes « STATUS »
15 consécutives par le dispositif hôte 10 correspond à l'intervalle d'accès t_{acc} (nommé en terminologie anglo-saxonne « *Polling Interval* »).

L'intervalle d'accès t_{acc} est associé au dispositif hôte 10, et sa valeur varie d'un dispositif hôte à un autre. Ainsi, un dispositif hôte 10 peut être caractérisé par rapport à cette valeur.

20 D'une manière générale, l'intervalle d'accès t_{acc} présente une valeur de 30 secondes, c'est-à-dire que 30 secondes s'écoulent entre deux accès du dispositif hôte 10 à l'élément sécurisé 20, ou entre l'envoi des deux commandes STATUS du dispositif hôte 10 à l'élément sécurisé 20.

L'intervalle d'accès t_{acc} peut être enregistré dans l'élément sécurisé
25 20 par exemple lors de sa fabrication.

Comme représenté sur la figure 3, un nombre déterminé d'intervalles d'accès t_{acc} est présent entre le moment où le dispositif hôte 10 va commencer à envoyer ses commandes STATUS (après sa phase d'allumage et d'initialisation, instant représenté par 0 sur la figure 3) et le premier instant de
30 connexion t_1 . Le temps écoulé entre l'instant 0 et le premier instant de connexion t_1 représente une période de temps nommée T_1 . On notera qu'un nombre déterminé d'intervalles d'accès t_{acc} est présent entre l'instant 0 et le

premier instant de connexion t_1 , dans cet exemple le nombre étant de neuf intervalles d'accès.

En outre, un nombre déterminé d'intervalles d'accès t_{acc} sont présents entre le premier instant de connexion t_1 et le deuxième instant de connexion t_2 , le temps écoulé entre le premier instant de connexion t_1 et le deuxième instant de connexion t_2 représente une période de temps nommée T_1' . Ainsi, la période de temps T_1' comprend un nombre déterminé d'intervalles d'accès t_{acc} . Dans l'exemple représenté, la période de temps réelle écoulée entre deux instants de connexion consécutifs t_1 et t_2 ou période de connexion T_1' comporte cinq intervalles d'accès t_{acc} .

Ainsi, un intervalle d'accès t_{acc} représente le temps écoulé entre deux accès consécutifs du dispositif hôte 10 à l'élément sécurisé 20.

Dans l'exemple de réalisation représenté à la figure 3, les instants de temps t_{acc1} , t_{acc2} représentent respectivement un premier accès et un second accès du dispositif hôte 10 à l'élément sécurisé 20.

Dans certains dispositifs hôte 10, la valeur de l'intervalle d'accès t_{acc} associée peut être modifiée à la demande de l'élément sécurisé 20 qu'il incorpore.

Pour que l'intervalle d'accès t_{acc} puisse être modifié, le dispositif hôte 10 doit supporter une fonctionnalité permettant la modification de la valeur de l'intervalle d'accès t_{acc} .

Lorsqu'un élément sécurisé 20 souhaite modifier et proposer une modification de la valeur de l'intervalle d'accès t_{acc} , il envoie une commande, par exemple une commande proactive du type « Intervalle d'accès » (« *Poll Interval* » en terminologie anglo-saxonne), au dispositif hôte 10.

On notera qu'une commande proactive correspond à une commande adressée par un élément sécurisé vers un dispositif hôte incorporant l'élément sécurisé.

Si le dispositif hôte 10 supporte une fonctionnalité permettant la modification de la valeur de l'intervalle d'accès t_{acc} , il répond à l'élément sécurisé en lui envoyant une commande nommée « *Terminal*

Response Command» dans laquelle la valeur maximale de l'intervalle d'accès supportée par le dispositif hôte 10 est incluse.

On notera que la valeur de l'intervalle d'accès t_{acc} est uniquement modifiée si le dispositif hôte supporte une fonctionnalité permettant cette
5 modification.

Dans certains cas, lorsque le dispositif hôte ne modifie pas la valeur de l'intervalle d'accès, il en informe l'élément sécurisé et celui-ci peut à son tour en informer le serveur.

Comme décrit ci-dessus, on notera que la période de temps réelle
10 entre deux instants de connexion consécutifs ou période de connexion est différente pour chaque élément sécurisé 20 de l'ensemble. Cette période de temps ou période de connexion étant déterminée entre autre en fonction d'un paramètre d'identification unique ICCID associé à l'élément sécurisé 20.

Comme illustré sur la figure 3, la période de connexion T ou période
15 de temps entre deux instants de connexion consécutifs t_1 , t_2 représente un temps équivalent à l'intervalle d'accès t_{acc} répété un certain nombre de fois.

Ainsi, la période de temps entre deux instants de connexion consécutifs t_1 , t_2 est fonction de la valeur de l'intervalle d'accès associé au
dispositif hôte 10.

Par conséquent, la période de temps entre deux instants de
20 connexion consécutifs t_1 , t_2 ou période de connexion T est déterminée dans un mode de réalisation par la formule :

$$T = n \times t_{acc}$$

où t_{acc} correspond à l'intervalle d'accès associé au dispositif hôte 10
25 incorporant l'élément sécurisé 20, et n au paramètre représentant le nombre de fois que l'intervalle d'accès t_{acc} est répété dans une période de temps entre deux instants de connexion t_1 , t_2 ou période de connexion T .

Le nombre de fois que l'intervalle d'accès t_{acc} est répété dans une période de connexion T correspond à la valeur d'un paramètre n . Le paramètre
30 n est déterminé en fonction du paramètre d'identification unique ICCID associé à l'élément sécurisé 20, ainsi que de deux paramètres, un premier paramètre V et un second paramètre I .

Ainsi, dans un mode de réalisation, la valeur du paramètre n est déterminée par une fonction F ayant comme entrées le paramètre d'identification unique ICCID, le premier paramètre V , et le deuxième paramètre I .

5 Ainsi, $n = F(ICCID, V, I)$

Les valeurs de paramètres ICCID, V et I sont stockées dans l'élément sécurisé 20 lors de sa fabrication. Le premier paramètre V et le deuxième paramètre I , par la suite, évoluent et sont mis à jour au cours de l'utilisation de l'élément sécurisé, une fois activé et déployé sur le « terrain ».

10 En particulier, la valeur du premier paramètre V est incrémentée après chaque connexion de l'élément sécurisé 20 au serveur 30. La valeur du deuxième paramètre I peut être modifiée par le serveur 30. Lorsque la valeur du deuxième paramètre I est modifiée par le serveur 30, la déduction par des dispositifs tiers des instants de connexion est rendue davantage difficile, les
15 connexions entre l'élément sécurisé et le serveur étant davantage sécurisées.

Ces paramètres peuvent être utilisés pour la détermination de la période de connexion T par l'élément sécurisé 20 sans nécessiter aucune action de la part du serveur 30.

20 Dans un mode de réalisation, la fonction $F(ICCID, V, I)$ prend la forme suivante :

$$F(ICCID, V, I) = \text{constante } 1 + (\text{hash}(ICCID, V, I)) \times \text{MODULO } \text{constante } 2$$

où *constante 1*, *constante 2* représentent des durées, le résultat de la fonction F étant ainsi un temps.

25 A titre d'exemple nullement limitatif, *constante 1* présente une valeur d'une semaine et *constante 2* d'un jour. L'élément sécurisé établit alors une connexion avec le serveur à des instants de connexion espacés d'une durée correspondant à une semaine plus une durée aléatoire entre 0 et 1 jour.

Bien entendu, les valeurs de *constante 1* et *constante 2* peuvent être différentes de l'exemple précédent.

30 Une fois que le paramètre n a été déterminé, l'intervalle d'accès t_{acc} est multiplié par la valeur déterminée, le résultat de cette multiplication étant la

période de temps entre deux instants de connexion consécutifs t_1 , t_2 ou période de connexion T .

Une fois la période de connexion T déterminée, des instants de connexion (tels que le premier instant de connexion t_1 et le second instant de connexion t_2 représentés à la figure 3) sont déterminés en fonction de la

L'élément sécurisé 20 établit une connexion avec le serveur 30 à chaque instant de connexion déterminé.

Ainsi, la période de temps entre deux instants de connexion consécutifs t_1 , t_2 est fonction d'un ensemble de paramètres et de l'intervalle d'accès t_{acc} associé au dispositif hôte 10, l'ensemble de paramètres comportant le paramètre d'identification unique ICCID, le premier paramètre V et le deuxième paramètre I .

On notera que l'élément sécurisé 20 et le serveur 30 déterminent les instants de connexion et la période de temps entre deux instants de connexion t_1 , t_2 théoriques en utilisant une valeur théorique d'intervalles d'accès t_{acc} .

Néanmoins, comme indiqué ci-dessus, la valeur réelle de l'intervalle d'accès du dispositif hôte 10 à l'élément sécurisé 20 ne correspond pas à celle demandée par l'élément sécurisé 20, cette valeur demandée étant celle utilisée dans le calcul de la période de temps théorique entre deux instants de connexion t_1 , t_2 consécutifs.

Ainsi, il existe un intervalle d'accès réel et un intervalle d'accès théorique, et par conséquent, une période de temps théorique et une période de temps réelle entre deux instants de connexion consécutifs.

Selon un mode de réalisation, dans l'élément sécurisé 20, un compteur de déclenchement est configuré pour compter le nombre d'intervalles d'accès t_{acc} présents dans la période de connexion T ou période de temps entre deux instants de connexion t_1 , t_2 consécutifs, et ainsi déterminer un instant de connexion au serveur 30.

Lorsqu'un nombre d'intervalles d'accès t_{acc} égal à la valeur du paramètre n déterminé est compté, l'élément sécurisé 20 établit une connexion avec le serveur 30 à l'instant de temps déterminé.

Comme indiqué ci-dessus, lors d'un accès du dispositif hôte 10 à l'élément sécurisé 20, par exemple à l'instant t_{acc1} , une commande « STATUS » est envoyée par le dispositif hôte 10 à l'élément sécurisé 20.

5 Ainsi, dans le mode de réalisation décrit, le compteur de déclenchement compte le nombre de commandes « STATUS » envoyées par le dispositif hôte 10 à l'élément sécurisé 20, ce qui correspond à compter le nombre d'intervalles d'accès t_{acc} réels.

Comme il sera décrit ultérieurement, selon un mode de réalisation, le compteur de déclenchement est incrémenté à chaque commande STATUS reçue.
10

Selon un autre mode de réalisation, le compteur de déclenchement est initialisé à la valeur du paramètre n qui a été déterminé, le compteur de déclenchement étant décrémenté à chaque commande STATUS reçue.

Des étapes du procédé de gestion de connexions entre un élément sécurisé 20 et un serveur 30 d'un réseau de communication 300 selon un mode de réalisation est représenté sur la Figure 4.
15

Lorsque le dispositif hôte 10 incorporant l'élément sécurisé 20 est allumé, une procédure d'initialisation E1 est mise en œuvre.

Pendant cette procédure d'initialisation, l'élément sécurisé 20 envoie
20 (après un possible délai, au serveur 30), par l'intermédiaire du dispositif hôte 10, un message lui indiquant qu'il est opérationnel et vient d'être activé, ce message comportant des paramètres. Ainsi, l'élément sécurisé 20 envoie une commande E10 contenant ces paramètres au dispositif hôte 10.

On notera que l'élément sécurisé peut attendre un délai après être allumé (« *power-on* » en terminologie anglo-saxonne) avant de se connecter au
25 serveur 30. Ce délai est déterminé en utilisant la fonction $F(ICCID, V, I)$, cette dernière permettant d'obtenir la valeur du paramètre n , et en utilisant la valeur de l'intervalle d'accès (« Polling interval »).

Pour la détermination du premier instant de connexion t_1 de
30 l'élément sécurisé 20 au serveur 30, les valeurs du premier paramètre V et du deuxième paramètre I sont telles que la valeur de ce premier instant de

connexion t1 est compris entre un premier instant de temps prédéterminé et un second instant de temps prédéterminé.

Les valeurs des premier et second paramètres (V, I) sont enregistrées dans l'élément sécurisé lors de sa fabrication et sont utilisés pour
5 la détermination du tout premier instant de connexion de l'élément sécurisé au serveur lors de la première mise en service de l'élément sécurisé. De même, premier instant de temps prédéterminé second instant de temps prédéterminé sont enregistrées dans l'élément sécurisé lors de sa fabrication.

Ainsi, selon un mode de réalisation, le procédé de gestion des
10 connexions comporte l'établissement d'une première connexion, à un premier instant de connexion, ayant une valeur comprise entre un premier instant de temps prédéterminé et un second instant de temps prédéterminé. Cette étape de détermination est mise en œuvre après la phase d'allumage ou de redémarrage et l'étape d'initialisation.

15 Les paramètres envoyés par l'élément sécurisé via la commande E10, pendant la procédure d'initialisation comportent par exemple le paramètre d'identification unique ICCID associé à l'élément sécurisé 20 ainsi que le profil du dispositif hôte 10, profil qui a été transmit au préalable à l'élément sécurisé par le dispositif hôte après allumage du dispositif hôte et durant la séquence
20 d'initialisation. Par profil, nous entendons les caractéristiques supportées par le dispositif hôte 10 (habituellement désignées en terminologie anglo-saxonne par le terme « *terminal profile* »).

Le dispositif hôte 10 envoie un message E11 au serveur 30 transférant ainsi les informations reçues en provenance de l'élément sécurisé
25 20 par le biais de la commande E10. Le serveur 30 accuse réception au dispositif hôte 10 avec un message E12, et le dispositif hôte 10 envoie l'accusé de réception via une commande E13 à l'élément sécurisé 20.

La procédure d'initialisation permet en particulier d'enregistrer le profil ou « terminal profile » du dispositif hôte 10 auprès du serveur 30. On
30 notera que l'ICCID est référencé préalablement dans les serveurs pour des aspects d'authentification dans le réseau. Ainsi, grâce à l'envoi de l'ICCID de l'élément sécurisé 20 en même temps que le profil, une correspondance entre

le profil du dispositif hôte 10 et l'élément sécurisé 20 qu'il contient est ainsi établie.

Ainsi, une fois que la procédure d'initialisation est terminée, l'élément sécurisé 20 et le dispositif hôte 10 sont enregistrés dans le serveur 30.

5 Ensuite, l'élément sécurisé 20 met en œuvre une étape d'envoi E2 du paramètre d'identification unique ICCID. Lors de cette étape d'envoi E2, une commande E20 est envoyée par l'élément sécurisé 20 au dispositif hôte 10. Le dispositif hôte 10 transfère alors les informations de la commande E20 au serveur 30 par l'intermédiaire du message E21. Le serveur 30 renvoie ensuite
10 un accusé de réception E22 au dispositif hôte 10, qui à son tour, envoie l'accusé de réception via une commande E23 à l'élément sécurisé 20.

Outre le paramètre d'identification unique ICCID, dans l'étape d'envoi E2, l'élément sécurisé 20 envoie au serveur (par le moyen du dispositif hôte 10) la dernière valeur du paramètre n atteinte à l'étape de comptage d'un nombre
15 d'intervalles d'accès réels, avant que ledit dispositif hôte 10 ne soit éteint ou redémarré.

Comme décrit ci-dessus, le procédé comporte une étape de détermination du temps réelle entre deux instants de connexion t_1 , t_2 consécutifs entre l'élément sécurisé 20 et le serveur 30.

20 Côté serveur 30, cette étape de détermination est mise en œuvre une fois que le serveur 30 a reçu deux connexions consécutives de la part de l'élément sécurisé 20.

Côté élément sécurisé 20, l'étape de détermination de cette période de temps réelle comporte une étape de comptage d'un nombre d'intervalles
25 d'accès réels t_{acc} du dispositif hôte 10 à l'élément sécurisé 20, la période de temps réelle étant équivalente au temps écoulé lors du comptage d'un nombre d'intervalles réels d'accès t_{acc} égal à la valeur du paramètre n déterminé.

La détermination de la valeur du paramètre n est mise en œuvre en utilisant l'ensemble de paramètres, l'ensemble de paramètres comportant un
30 paramètre d'identification unique ICCID, un premier paramètre V et un second paramètre I .

On notera que l'envoi des commandes E20, E21, E22 et E23 est optionnel, cet envoi étant seulement mis en œuvre selon certains modes de réalisation.

Dans un mode de réalisation, le procédé comporte la création E40
5 d'une structure de données comportant des données relatives à un ensemble d'éléments sécurisés 20, les données relatives à l'ensemble d'éléments sécurisés 20 étant pour chaque élément sécurisé 20 de l'ensemble, la période de temps théorique déterminée, la période de temps réelle déterminée, l'intervalle d'accès théorique déterminé, l'intervalle d'accès réel déterminé et le
10 nombre d'intervalles d'accès comptés lors de l'étape de comptage.

Selon un mode de réalisation, la structure de données est stockée dans le serveur 30, et est mise à jour lorsqu'au moins une des données est déterminée.

La structure de données comporte en outre le paramètre
15 d'identification unique de l'élément sécurisé 20, le profil du dispositif hôte 10 (« *terminal profile* » en terminologie anglo-saxonne), le premier instant de temps prédéterminé et le second instant prédéterminé (l'élément sécurise établissant la première connexion au serveur à un instant compris entre ces deux instant de temps prédéterminés) et la valeur du compteur de
20 déclenchement. Une association entre un élément sécurisé référencé par son identifiant unique ICCID et les caractéristiques des paramètres du dispositif hôte dans lequel il se trouve ou bien les caractéristiques de l'élément sécurisé lui-même peut ainsi être faite. De même, une association entre un dispositif hôte donné et les caractéristiques des paramètres de ce type de dispositif hôte
25 peut aussi être faite.

La structure de données comporte aussi la valeur du paramètre n déterminé. Cette valeur du paramètre n est mise à jour à chaque étape de détermination E100 de la valeur du paramètre.

En outre, lors de la première mise en fonctionnement de l'élément
30 sécurisé la valeur du paramètre n déterminée après la phase d'initialisation E1 est stockée dans la structure de données. Cette première valeur du paramètre

n peut être utilisée par la suite par le serveur dans une mode de fonctionnement.

Dans le mode de réalisation représenté, l'élément sécurisé 20 demande au dispositif hôte 10 de modifier l'intervalle d'accès t_{acc} . L'élément sécurisé 20 envoie ainsi une commande $E_{t_{acc}}$, (commande proactive de type « *Poll Interval* » en terminologie anglo-saxonne) au dispositif hôte 10 et le dispositif hôte 10 lui répond avec l'envoi d'une commande ER (commande « *Terminal Response* » en terminologie anglo-saxonne).

Ces étapes de demande de modification du « *Polling interval* » sont connues de l'homme du métier et ne sont pas décrites ici en détail.

On notera que dans certains dispositifs hôte 10, l'intervalle d'accès t_{acc} peut être modifié à la demande de l'élément sécurisé 20. Néanmoins, dans d'autres dispositifs hôte 10, l'intervalle d'accès n'est pas modifiable et/ou la demande de modification de la part de l'élément sécurisé n'est pas prise en compte par le dispositif hôte.

Une fois que le dispositif hôte 10 est allumé, il va envoyer périodiquement à l'élément sécurisé 20 des commandes « STATUS » E30, E30' et 30''.

Dans ce mode de réalisation, une fois que le compteur de déclenchement atteint à l'étape de comptage, un nombre déterminé de commandes « STATUS » envoyées du dispositif hôte 10 à l'élément sécurisé 20, l'élément sécurisé 20 lance une connexion avec le serveur 30 par l'intermédiaire du dispositif hôte 10.

Selon un mode de réalisation, le compteur de déclenchement peut être incrémenté et lorsqu'il atteint la valeur du paramètre n , l'élément sécurisé 20 lance une connexion, par exemple une connexion OTA (« *Over The Air* » en terminologie anglaise), par l'intermédiaire du dispositif hôte 10 avec le serveur 30.

Selon un autre mode de réalisation, le compteur de déclenchement peut être initialisé à la valeur du paramètre n , et il sera par la suite décrémenté à chaque réception d'une commande « STATUS ». Une fois que le compteur de déclenchement présente la valeur zéro (la valeur du paramètre n ayant été ainsi

comptée), l'élément sécurisé 20 lance une connexion avec le serveur 30 par l'intermédiaire du dispositif hôte 10. Cette connexion est par exemple une connexion OTA (« *Over The Air* » en terminologie anglaise).

Pour ce faire, l'élément sécurisé 20 envoie une commande de connexion E31 au dispositif hôte 10 qui envoie alors un message de connexion E32 au serveur 30.

Le serveur 30, de son côté, comprend des moyens de détermination d'un paramètre n dont la valeur est fonction dudit paramètre d'identification unique ICCID, d'un premier paramètre V et d'un second paramètre I .

Le serveur 30 comprend aussi des moyens de détermination des instants de connexion théoriques consécutifs de l'élément sécurisé 20 avec le serveur 30. Lesdits instants de connexions théoriques sont déterminés par la multiplication d'un intervalle d'accès théorique associé à un dispositif hôte 10 incorporant ledit élément sécurisé 20 et représentent le temps écoulé théorique entre deux accès consécutifs dudit dispositif hôte 10 audit élément sécurisé 20, par ladite valeur du paramètre n déterminée.

Aussi, à titre d'exemple, nullement limitatif, la valeur de l'intervalle d'accès théorique peut être de 30 secondes.

Ainsi, le serveur 30 met en œuvre une étape de détermination E300 d'une période de temps théorique entre deux instants de connexion t_1 , t_2 consécutifs entre l'élément sécurisé 20 et le serveur 30 en fonction d'un ensemble de paramètres et d'un intervalle d'accès théorique associé au dispositif hôte 10.

Cette étape de détermination E300 de ladite période de temps théorique comporte une étape de multiplication dudit intervalle d'accès théorique par ladite valeur dudit paramètre n déterminée, le résultat étant ladite période de temps théorique T . Dans certains modes de réalisation, la valeur du compteur reçu par le serveur est prise en compte dans la détermination des instants de connexion t_1 , t_2 , ..., t_n .

Dans d'autres modes de réalisation, le serveur 30 met en œuvre une étape de détermination E100 de la valeur du paramètre n en utilisant l'ensemble de paramètres ICCID, V , I .

Dans un mode de réalisation, les valeurs du premier paramètre V et du second paramètre I sont modifiées à des instants prédéfinis.

Par exemple, les valeurs des paramètres V, I sont modifiées par le serveur à chaque connexion entre l'élément sécurisé 20 et le serveur 30. Les
5 instants auxquels des connexions entre l'élément sécurisé 20 et le serveur 30 sont mises en œuvre correspondent ainsi à des instants prédéfinis.

Ainsi, une fois que la connexion entre l'élément sécurisé 20 et le serveur 30 est établie, le serveur 30 peut envoyer de nouveaux paramètres V, I au dispositif hôte 10 via un message E33. Le dispositif hôte 10 transfère alors, à
10 son tour et via la commande E34 destinée à l'élément sécurisé 20, les paramètres V, I modifiés.

Une fois la commande E34 reçue par l'élément sécurisé 20, l'élément sécurisé 20 détermine la valeur du paramètre n, en fonction du paramètre d'identification unique ICCID, et du premier paramètre V et second
15 paramètre I modifiés. Ensuite, l'élément sécurisé 20 détermine une nouvelle période de connexion mettant en œuvre une étape de comptage de la valeur du paramètre n déterminé.

L'élément sécurisé 20 réinitialise alors la valeur du compteur de déclenchement à la valeur du paramètre n déterminée, et compte à nouveau le
20 nombre de commandes « STATUS » E30, E30', E30'' reçues de la part du dispositif hôte 10. Une fois comptabilisé un nombre de commandes « STATUS » E30, E30', E30'', équivalant à la valeur du paramètre n, l'élément sécurisé 20 lance une nouvelle connexion avec le serveur 30.

Ainsi, l'élément sécurisé 20 envoie une nouvelle commande de
25 connexion E31' au dispositif hôte 10, et le dispositif hôte 10 transfère la commande de connexion via un message E32' au serveur 30. Le serveur 30 peut ensuite envoyer au dispositif hôte 10 un message E33' comportant une mise à jour du premier paramètre V et du second paramètre I. Le dispositif hôte 10, transfère alors à l'élément sécurisé 20 les paramètres V, I mis à jour via une
30 commande E34'.

L'élément sécurisé 20 détermine ensuite la valeur du paramètre n avec le paramètre d'identification unique ICCID et le premier paramètre V et le

second paramètre I mis à jour, afin de déterminer la nouvelle période de connexion $T1'$.

On notera que les périodes de connexion $T1$, $T1'$ peuvent être différentes ou égales dès lors que le premier paramètre V et le second paramètre I ont été mis à jour par le serveur 30. Bien entendu, si au moins un des paramètres V , I est modifié, lors de leur mise à jour par le serveur, par une valeur différente de la précédente, la période de connexion $T1'$ sera différente de la période de connexion $T1$. Au contraire, si aucun des paramètres V , I n'est modifié lors de leur mise à jour par le serveur, ou s'ils le sont mais avec des valeurs identiques aux précédentes, la période de connexion $T1'$ sera égale à la période de connexion $T1$.

Quant à l'intervalle d'accès t_{acc} , il n'a pas été modifié entre deux connexions consécutives.

Comme indiqué ci-dessus, la mise à jour périodique des premier et second paramètres V , I renforce la sécurité dans les connexions entre l'élément sécurisé 20 et le serveur 30, les périodes de connexions $T1$, $T1'$ associées aux éléments sécurisés 20 étant difficilement prédictibles par un dispositif tiers.

Une fois que le serveur 30 a reçu deux connexions à des instants de connexion consécutifs t_1 , t_2 de la part de l'élément sécurisé 20, il est en mesure de mettre en œuvre l'étape de détermination E400 de la période de temps réelle entre deux instants de connexion consécutifs entre l'élément sécurisé 20 et le serveur 30.

Le procédé comporte ensuite une étape de détermination, mise en œuvre par ledit serveur 30, dudit intervalle d'accès réel associée audit dispositif hôte 10.

Dans un mode de réalisation, l'intervalle d'accès réel est déterminé à partir de ladite période de temps réelle et de ladite valeur dudit paramètre n déterminée.

Ensuite, le serveur 30 met en œuvre une étape de comparaison E500 de la période de temps théorique déterminée avec la période de temps réelle déterminée.

Si la période de temps théorique déterminée est différente de la période de temps réelle déterminée, le serveur met en œuvre une étape de modification E600 d'au moins un paramètre de l'ensemble des paramètres de sorte que la période de temps théorique présente une valeur proche de la période de temps réelle déterminée. Une fois les paramètres modifiés, une
5 étape de détermination E300 d'une nouvelle période de temps théorique prenant en compte ledit au moins un des paramètres modifiés est mise en œuvre.

Selon le mode de réalisation représenté, l'étape de modification
10 E600 est mise en œuvre par le serveur 30. Le procédé comporte alors en outre une étape d'envoi E33', mise en œuvre par le serveur, dans laquelle ledit au moins un paramètre V, I de l'ensemble de paramètres V, I, ICCID modifié est envoyé à l'élément sécurisé 20, l'étape de détermination E100 de la valeur d'un paramètre n étant mise en œuvre par l'élément sécurisé en utilisant ledit au
15 moins un paramètre V, I modifié reçu. L'élément sécurisé 20 détermine ensuite une nouvelle période de temps théorique en utilisant la valeur du paramètre n déterminé.

Selon un autre mode de réalisation (non représenté), l'étape de modification et l'étape de détermination d'une nouvelle période de temps
20 théorique sont mises en œuvre par ledit serveur 30. Le procédé comporte alors en outre une étape d'envoi, mise en œuvre par le serveur 30, dans laquelle la nouvelle période de temps théorique déterminée est envoyée à l'élément sécurisé 20.

REVENDICATIONS

1. Procédé de gestion des connexions entre un élément sécurisé et un serveur (30) d'un réseau de communication, ledit élément sécurisé (20) étant incorporé dans un dispositif hôte (10), ledit procédé de gestion des connexions étant caractérisé en ce qu'il comporte les étapes suivantes :
- détermination (E300) d'une période de temps théorique entre deux instants de connexion consécutifs entre ledit élément sécurisé et ledit serveur en fonction d'un ensemble de paramètres et d'un intervalle d'accès théorique associé audit dispositif hôte,
 - détermination (E400) d'une période de temps réelle entre deux instants de connexion consécutifs entre ledit élément sécurisé et ledit serveur,
 - comparaison (E500) de ladite période de temps théorique déterminée avec la période de temps réelle déterminée, et
 - si la période de temps théorique déterminée est différente de la période de temps réelle déterminée :
 - modification (E600) d'au moins un paramètres dudit ensemble des paramètres de sorte que la période de temps théorique présente une valeur proche de la période de temps réelle déterminée, et
 - détermination d'une nouvelle période de temps théorique prenant en compte ledit au moins un des paramètres modifié.
2. Procédé conforme à la revendication 1, caractérisé en ce qu'il comporte une étape de détermination (E100) de la valeur d'un paramètre n en utilisant ledit ensemble de paramètres (ICCID, V, I).
3. Procédé conforme à la revendication 2, caractérisé en ce que la détermination (E300) de ladite période de temps théorique comporte une étape de multiplication dudit intervalle d'accès théorique par ladite valeur dudit paramètre n déterminée, le résultat étant ladite période de temps théorique (T).
4. Procédé conforme à l'une des revendications 2 ou 3, caractérisé en ce que ladite étape de détermination de ladite période de temps réelle comporte une étape de comptage, mise en œuvre par ledit élément sécurisé (20), d'un nombre d'intervalles d'accès réels (t_{acc}) du dispositif hôte

(10) à l'élément sécurisé (20), la période de temps réelle étant équivalente au temps écoulé lors du comptage d'un nombre d'intervalles réels d'accès (t_{acc}) égal à la valeur du paramètre n déterminé.

5 5. Procédé conforme à la revendication 4, caractérisé en ce qu'il
comporte une étape d'envoi (E20), mise en œuvre par l'élément sécurisé (20),
dans laquelle la dernière valeur dudit paramètre n atteinte à l'étape de
comptage d'un nombre d'intervalles d'accès réels avant que ledit dispositif hôte
ne soit éteint ou redémarré, est envoyée au serveur, , ladite étape d'envoi (E20)
étant mise en œuvre lorsque ledit dispositif hôte (10) initie une phase
10 d'initialisation (E1) avec le serveur (30), ladite phase d'initialisation (E1) étant
mise en œuvre après l'allumage ou le redémarrage dudit dispositif hôte.

6. Procédé de gestion des connexions conforme à l'une des
revendications 1 à 5, caractérisé en ce que ledit ensemble de paramètres
comporte un paramètre d'identification unique (ICCID), un premier paramètre
15 (V) et un second paramètre (I).

7. Procédé de gestion des connexions conforme à la
revendication 6 caractérisé en ce que après la phase d'allumage ou de
redémarrage et la phase d'initialisation (E1), ledit procédé comporte
l'établissement d'une première connexion à un premier instant de connexion
20 ayant une valeur comprise entre un premier instant de temps prédéterminée et
un second instant de temps prédéterminé.

8. Procédé de gestion des connexions conforme à l'une des
revendications 4 à 7, caractérisé en ce qu'il comporte une étape de
détermination, mise en œuvre par ledit serveur, dudit intervalle d'accès réel
25 associée audit dispositif hôte à partir de ladite période de temps réelle et de
ladite valeur dudit paramètre n déterminée.

9. Procédé conforme à l'une des revendications 1 à 8, caractérisé
en ce que ladite étape de modification est mise en œuvre par le serveur, ledit
procédé comportant en outre une étape d'envoi (E33'), mise en œuvre par le
30 serveur (30), dans laquelle ledit au moins un paramètre (V, I) de l'ensemble de
paramètres (V, I, ICCID) modifié est envoyé audit élément sécurisé, ladite étape
de détermination d'une nouvelle période de temps théorique étant mise en

œuvre par ledit élément sécurisé (20) en utilisant ledit au moins un paramètre (V, I) modifié reçu.

10. Procédé conforme à l'une des revendications 2 à 5, caractérisé en ce que ladite étape de modification (E600) et ladite étape de détermination
5 (E100) de la valeur d'un paramètre n sont mises en œuvre par ledit serveur (30), ledit procédé comportant en outre une étape d'envoi, mise en œuvre par le serveur, dans laquelle ladite valeur du paramètre n déterminée est envoyée audit élément sécurisé.

11. Procédé de gestion des connexions conforme à l'une des
10 revendication 4 à 10, caractérisé en ce qu'il comporte la création (E40) d'une structure de données comportant des données relatives à un ensemble d'éléments sécurisés, lesdites données relatives audit ensemble d'éléments sécurisé étant pour chaque élément sécurisé de l'ensemble, ladite période de
15 temps théorique déterminée, ladite période de temps réelle déterminée, l'intervalle d'accès théorique déterminé, l'intervalle d'accès réel déterminé et le nombre d'intervalles d'accès comptés lors de l'étape de comptage.

12. Procédé de gestion des connexions conforme à la revendication 11, caractérisé en ce que ladite structure de données est stockée dans ledit serveur, et est mise à jour lorsqu'au moins une des données est
20 déterminée ou reçue.

13. Serveur d'un réseau de communication comportant des moyens de connexion avec un ensemble d'éléments sécurisés (20), chaque élément sécurisé étant incorporé dans un dispositif hôte, ledit serveur étant caractérisé en ce qu'il comporte pour chaque élément sécurisé (20):

25 - des moyens de détermination d'une période de temps théorique entre deux instants de connexion consécutifs entre ledit élément sécurisé et ledit serveur en fonction d'un ensemble de paramètres et d'un intervalle d'accès théorique associé audit dispositif hôte,

- des moyens de détermination d'une période de temps réelle entre
30 deux instants de connexion consécutifs entre ledit élément sécurisé et ledit serveur,

- des moyens de comparaison de ladite période de temps théorique déterminée avec la période de temps réelle déterminée, et

- des moyens de modification d'au moins un paramètres dudit ensemble des paramètres de sorte que la période de temps théorique présente une valeur proche de la période de temps réelle déterminée si la période de temps théorique déterminée est différente de la période de temps réelle déterminée, et

- des moyens de détermination d'une nouvelle période de temps théorique prenant en compte ledit au moins un des paramètres modifié.

10 14. Serveur conforme à la revendication 13, caractérisé en ce qu'il comporte en outre des moyens de détermination de la valeur d'un paramètre n en utilisant ledit ensemble de paramètres (ICCID, V, I), ledit ensemble de paramètres comportant un paramètre d'identification unique (ICCID), un premier paramètre (V) et un second paramètre (I).

15 15. Serveur conforme à la revendication 14, caractérisé en ce que lesdits moyens de détermination de ladite période de temps théorique comportent des moyens de multiplication dudit intervalle d'accès théorique par ladite valeur dudit paramètre n déterminée, le résultat de la mise en œuvre desdits moyens de multiplication étant ladite période de temps théorique (T).

20 16. Serveur conforme à la revendication 15, caractérisé en ce qu'il comporte des moyens de réception de la dernière valeur dudit paramètre n atteinte par des moyens de comptage d'un nombre d'intervalles d'accès réelles dans ledit élément sécurisé, avant que ledit dispositif hôte ne soit éteint ou redémarré, ladite dernière valeur dudit paramètre n étant envoyée par ledit
25 élément sécurisé lorsque ledit dispositif hôte (10) initie une phase d'initialisation avec le serveur, ladite phase d'initialisation étant mise en œuvre après l'allumage ou le redémarrage dudit dispositif hôte.

 17. Serveur conforme à la revendication 14, caractérisé en ce qu'il comporte des moyens de détermination dudit premier paramètre (V) et dudit
30 second paramètre (I) de sorte que ledit premier instant de connexion est dans une plage de valeurs comprise entre un premier instant de temps prédéterminée et un second instant prédéterminé.

18. Serveur conforme à l'une des revendications 16 à 17, caractérisé en ce qu'il comporte des moyens de détermination dudit intervalle d'accès réel associée audit dispositif hôte à partir de ladite période de temps réelle et de ladite valeur dudit paramètre n déterminée.

5 19. Serveur conforme à l'une des revendications 13 à 18, caractérisé en ce qu'il comporte des moyens d'envoi configurés pour envoyer audit élément sécurisé ledit au moins un paramètre (V, I) de l'ensemble de paramètres (V, I, ICCID) modifié.

20. 20. Serveur conforme à la revendication 19, caractérisé en ce que
10 lesdits moyens d'envoi sont en outre configurés pour envoyer audit élément sécurisé ladite nouvelle période de temps théorique déterminée.

21. 21. Serveur conforme à l'une des revendication 16 à 20, caractérisé en ce qu'il comporte des moyens de création d'une structure de données comportant des données relatives à un ensemble d'éléments
15 sécurisés, lesdites données relatives audit ensemble d'éléments sécurisé étant pour chaque élément sécurisé de l'ensemble, ladite période de temps théorique déterminée, ladite période de temps réelle déterminée, l'intervalle d'accès théorique, l'intervalle d'accès réel déterminé et le nombre d'intervalles d'accès comptés lors de l'étape de comptage.

20 22. Élément sécurisé comprenant des moyens de gestion des connexions avec un serveur (30) d'un réseau de communication (300), caractérisé en ce qu'il comporte en outre :

- des moyens de détermination de la valeur d'un paramètre n en utilisant un ensemble de paramètres (V, I, ICCID), ledit ensemble de
25 paramètres comportant un paramètre d'identification unique (ICCID) associé audit élément sécurisé (20), un premier paramètre (V) et un second paramètre (I),

- des moyens de détermination de la période de temps réelle entre deux instant de connexion consécutifs (t_1 , t_2) au serveur (30), et

30 - des moyens d'établissement d'une connexion avec le serveur (30) à des instants de connexion (t_1 , t_2 , ..., t_n).

23. Élément sécurisé conforme à la revendication précédente, caractérisé en ce que lesdits moyens de détermination de ladite période de temps réelle comporte des moyens de comptage d'un nombre d'intervalles d'accès réelles (t_{acc}) du dispositif hôte à l'élément sécurisé, la période de temps réelle étant équivalente au temps écoulé lors du comptage d'un nombre d'intervalles réelles d'accès (t_{acc}) égal à la valeur du paramètre n déterminé par les moyens de détermination.

24. Élément sécurisé conforme à l'une des revendications 22 ou 23, caractérisé en ce qu'il est un élément sécurisé de type UICC ou un élément sécurisé de type UICC embarqué (eUICC) ou un élément sécurisé embarqué (eSE).

25. Dispositif hôte caractérisé en ce qu'il comporte un élément sécurisé conforme à l'une des revendications 22 à 24.

26. Programme d'ordinateur comprenant des instructions pour la mise en œuvre d'un procédé selon l'une des revendications 1 à 12, lorsqu'il est chargé et exécuté par un microprocesseur.

27. Support d'informations lisible par un microprocesseur, comprenant les instructions d'un programme d'ordinateur pour mettre en œuvre un procédé selon l'une des revendications 1 à 12.

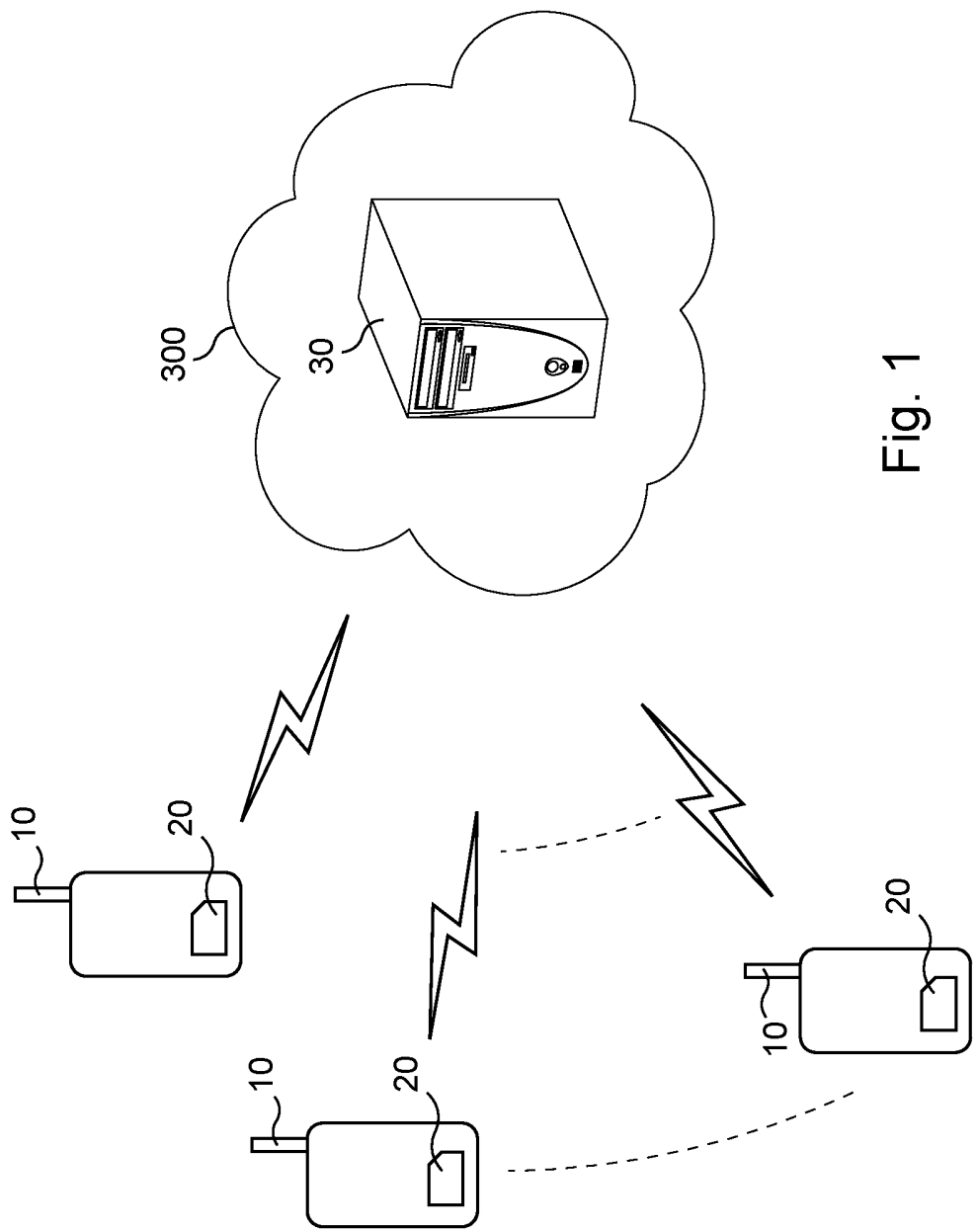
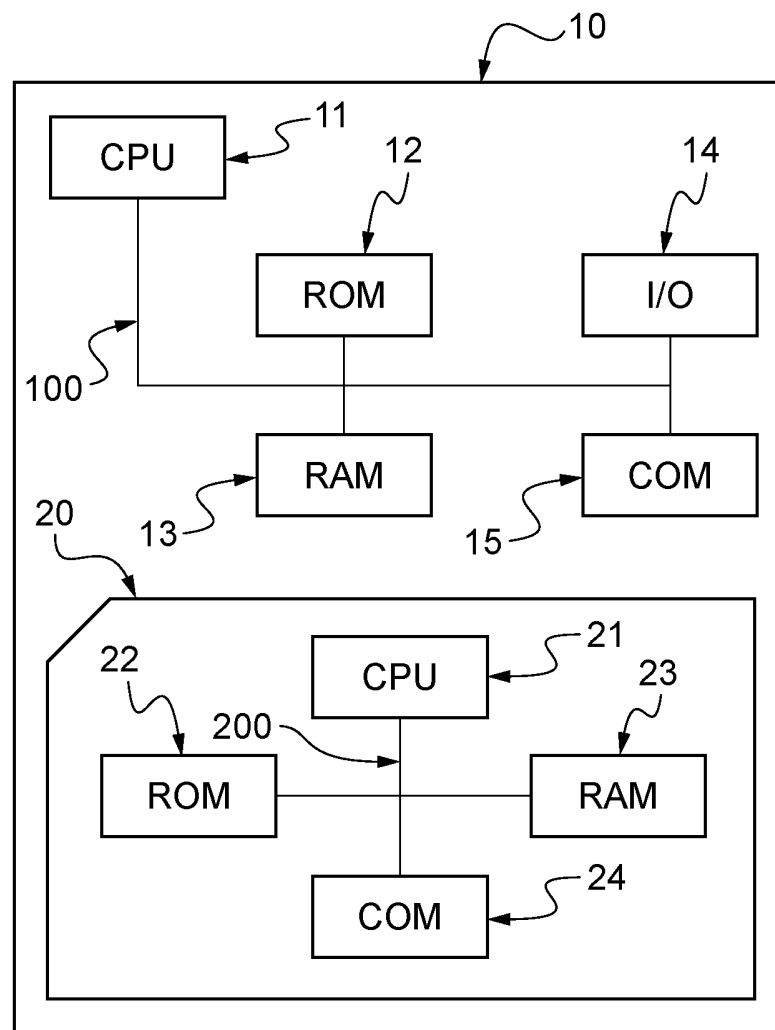


Fig. 1

2/4

Fig.2



3/4

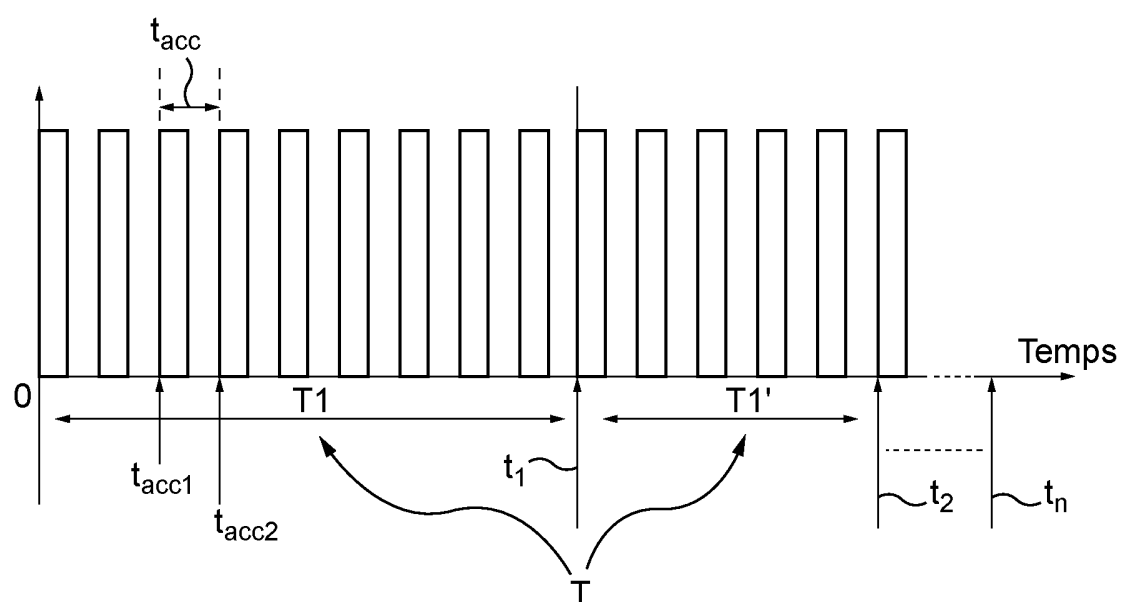
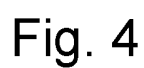


Fig. 3





RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement
national

FA 822109
FR 1562872

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	US 2015/059006 A1 (WHITE BRIAN M [US]) 26 février 2015 (2015-02-26)	22-25	H04W76/02
A	* alinéa [0017]; figure 1 * * alinéa [0038] - alinéa [0046] *	1-21, 26, 27	H04W4/00 H04L29/06
A	Giesecke & Devrient: "White Paper The OTA Platform in the World of LTE", 1 janvier 2011 (2011-01-01), XP055111231, Extrait de l'Internet: URL: http://www.carabinerpr.com/pdf/WP_OTA_and_LTE_Jan_11.pdf [extrait le 2014-04-01] * le document en entier *	1-27	
A	GLOBALPLATFORM: "Remote Application Management over HTTP Card Specification v2.2 - Amendment B Version 1.1", INTERNET CITATION, juin 2009 (2009-06), pages 1-25, XP002590002, Extrait de l'Internet: URL: http://www.globalplatform.org/specificationscard.asp [extrait le 2010-06-30] * alinéa [04.5] *	1-27	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			H04W H04L G06F G07F
Date d'achèvement de la recherche		Examineur	
25 juillet 2016		Figiel, Barbara	
CATÉGORIE DES DOCUMENTS CITÉS		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	
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			

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE

RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 1562872 FA 822109

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 25-07-2016

Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2015059006 A1	26-02-2015	AUCUN	