(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 892 876**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **05 11124**

(51) Int Cl[8] : **H 04 L 9/14** (2006.01)

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 02.11.05.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 04.05.07 Bulletin 07/18.

(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 :**

(71) **Demandeur(s) :** *GEMPLUS Société anonyme* — FR.

(72) **Inventeur(s) :** BRIER ERIC et CIET MATHIEU.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** NOVAGRAAF TECHNOLOGIES (CABINET BALLOT).

(54) PROCEDE DE DEPOT SECURISE DE DONNEES NUMERIQUES, PROCEDE ASSOCIE DE RECUPERATION DE DONNEES NUMERIQUES, DISPOSITIFS ASSOCIES POUR LA MISE EN OEUVRE DES PROCEDES, ET SYSTEME COMPRENANT LES DITS DISPOSITIFS.

(57) L'invention concerne un procédé de dépôt sécurisé de données (DATA), au cours duquel un déposant (A) chiffre les données (DATA) avec une clé de transfert (RAND) et chiffre la clé de transfert avec une clé d'un tiers de confiance (B), puis dépose les données chiffrées et la clé de transfert chiffrée sur un support de stockage (D).

L'invention concerne également un procédé de récupération de données (DATA), au cours duquel un destinataire des données récupère le contenu du support de stockage, s'authentifie auprès du tiers de confiance, et lui transmet la clé de transfert chiffrée. Après avoir authentifié le destinataire, le tiers de confiance lui retourne la clé de transfert déchiffrée. Le destinataire peut alors récupérer les données (DATA).

L'invention concerne enfin des dispositifs pour la mise en oeuvre des procédés ci-dessus.

- s'authentifie 'authentifier uthentifie s'authentifie
- s'authentifie

FR 2 892 876 - A1

Procédé de dépôt sécurisé de données, procédé associé de récupération de données, dispositifs associés pour la mise en œuvre des procédés,et système comprenant les dits dispositifs

L'invention concerne le dépôt sécurisé de données par un déposant sur un support de stockage éventuellement non sécurisé, et la récupération ultérieure de ces données par un destinataire éventuellement inconnu du déposant, ou inexistant au moment du dépôt. Les données sont des données numériques, ou bien des données analogiques numérisées.

Des solutions connues à ce problème consistent à passer par l'intermédiaire d'un tiers de confiance.

Une première solution, connue sous le nom de délégation totale, consiste pour le déposant à chiffrer les données avec une clé d'un tiers de confiance et à transmettre les données chiffrées au tiers de confiance. Pour récupérer les données ultérieurement, le destinataire s'authentifie auprès du tiers de confiance qui lui transmet en retour les données qu'il a préalablement déchiffrées avec sa clé puis éventuellement chiffré avec une clé fournie par le destinataire.

Une deuxième solution, connue sous le nom de délégation de droit, consiste pour le déposant à, d'une part, chiffrer les données avec une clé de transfert et mémoriser les données chiffrées sur un support de stockage accessible au destinataire et, d'autre part, à chiffrer la clé de transfert avec la clé du tiers de confiance et à transmettre la clé de transfert chiffrée au tiers de confiance. Pour récupérer les données ultérieurement, le destinataire s'authentifie auprès du tiers de confiance qui lui transmet en retour la clé de transfert qu'il a préalablement déchiffrée avec sa clé puis éventuellement chiffrée avec une clé fournie par le

destinataire. Le destinataire va ensuite récupérer les données chiffrées sur le support de stockage, puis les déchiffre avec la clé de transfert qu'il a obtenue du tiers de confiance.

Le chiffrement des données et / ou de la clé de transfert peut être réalisé soit par un procédé de chiffrement symétrique soit par un procédé de chiffrement asymétrique.

Les solutions connues décrites ci-dessus présentent plusieurs inconvénients.

Un canal de communication est nécessaire entre le déposant et le tiers de confiance, pour transmettre les données ou au moins une clé de transfert.

Dans la mesure où le déposant transmet des informations (données ou clé de transfert) au tiers de confiance, l'anonymat du déposant n'est pas garanti.

Le tiers de confiance doit conserver des informations, des données ou au moins une clé de transfert, pour une durée inconnue et éventuellement illimitée si le destinataire ne vient pas récupérer les données. Ceci est peu réaliste s'il y a un très grand nombre de déposants et / ou de grands volumes de données à conserver.

Enfin, dans le cas d'une délégation totale, le tiers de confiance a un accès en clair aux données à transmettre.

L'invention a pour objet un procédé de dépôt sécurisé de données et un procédé de récupération de données qui ne présentent pas les inconvénients cités ci-dessus des procédés connus. L'invention a également pour objet des dispositifs pour la mise en œuvre des procédés de l'invention.

Plus précisément, l'invention a pour objet un procédé de dépôt sécurisé de données, au cours duquel un déposant

chiffre les données avec une clé de transfert et chiffre la clé de transfert avec une clé d'un tiers de confiance, puis dépose les données chiffrées et la clé de transfert chiffrée sur un support de stockage.

L'invention concerne également un procédé de récupération de données, au cours duquel :

- un destinataire récupère sur un support de stockage des données chiffrées avec une clé de transfert, et une clé de transfert chiffrée avec une clé d'un tiers de confiance,
- le destinataire s'authentifie auprès du tiers de confiance,
- le destinataire envoie la clé de transfert chiffrée au tiers de confiance,
- après authentification du destinataire, le tiers de confiance déchiffre la clé de transfert chiffrée avec sa clé et renvoie la clé de transfert au destinataire,
- le destinataire déchiffre les données chiffrées avec la clé de transfert.

L'invention concerne encore un dispositif de dépôt sécurisé de données, comprenant :

- un générateur de nombre aléatoire pour générer une clé de transfert aléatoire (RAND),
- un premier moyen de calcul pour chiffrer des données (DATA) avec la clé de transfert,
- un deuxième moyen de calcul pour chiffrer la clé de transfert avec une clé d'un tiers de confiance, et
- un moyen pour mémoriser les données chiffrées et la clé de transfert chiffrée sur un support de stockage accessible à un destinataire des données.

Ainsi, et comme on le verra mieux dans l'exemple décrit plus loin, lors du dépôt des données selon le procédé sécurisé de l'invention, le déposant n'a aucun contact avec le tiers de confiance et ne lui transmet aucune information, même pas une clé. En conséquence, aucun

canal de communication n'est nécessaire entre le déposant et le tiers de confiance et l'anonymat du déposant est garanti vis-à-vis du tiers de confiance. De plus, le tiers de confiance n'a pas de données à conserver ni d'informations sur les données. Il peut même ne pas avoir connaissance du fait qu'un destinataire viendra peut-être un jour le contacter. Enfin, le tiers n'a pas accès en clair aux données, à moins qu'il n'ait un accès physique au support de stockage des données.

L'invention sera mieux comprise, et d'autres caractéristiques et avantages de l'invention ressortiront clairement de la description qui en est faite ci-après, à titre indicatif et nullement limitatif. La description est à lire en référence aux figures suivantes :

- la figure 1 est un organigramme d'un procédé de dépôt sécurisé selon l'invention,
- la figure 2 est un organigramme d'un procédé de récupération de données, selon l'invention, et
- la figure 3 est un exemple de système mettant en œuvre le procédé de dépôt selon la figure 1 et le procédé de récupération selon la figure 2.

La figure 3 représente un système susceptible d'être utilisé pour la mise en œuvre des procédés selon l'invention dans le domaine de la communication mobile.

Plus précisément, le système de la figure 3 permet à un premier utilisateur disposant d'un équipement mobile 1 avec un accès sur un réseau de communication 2 et d'un module 3 d'authentification personnelle, d'autoriser un deuxième utilisateur (ou le même premier utilisateur) à utiliser l'équipement mobile 1 avec un deuxième module d'authentification 4 pour accéder au réseau de communication 2. Pour cela, sur demande du premier

utilisateur, le premier module d'authentification dépose de manière sécurisée dans une mémoire de l'équipement mobile des données nécessaires pour accéder au réseau 2. Le système permet ainsi le transfert sécurisé de données du premier module vers le deuxième module par l'intermédiaire de la mémoire de l'équipement mobile.

Selon le réseau de communication auquel les utilisateurs ont accès, l'équipement mobile est un téléphone mobile, un terminal, un PC personnel, etc., et le module d'authentification personnelle est une carte UICC (Universal Integrated Circuit Card) munie d'une application SIM (Subscriber Identity Module), USIM (Universal Subscriber Module) ou ISIM (IP Multimedia Services Identity Module).

La figure 1 représente un organigramme général du procédé de dépôt selon l'invention. Dans une première étape, un déposant A chiffre des données DATA avec une clé de transfert RAND, et chiffre la clé de transfert RAND avec une clé publique pkB d'un tiers de confiance B. Dans une deuxième étape, A mémorise ensuite les données chiffrées $E_{RAND}(DATA)$ et la clé de transfert chiffrée $E_{pkB}(RAND)$ sur un support de stockage.

Dans l'exemple représenté sur la figure 3, le déposant A est un premier module 3 d'authentification d'utilisateur. Le tiers de confiance B est un opérateur exploitant un réseau de communication mobile 2. Le mot "exploitant" doit être ici compris au sens le plus large. L'exploitant peut être une personne morale propriétaire du réseau, ou locatrice du réseau, ou même une personne morale qui sous-traite l'exploitation du réseau à une autre personne. Le support de stockage D est une mémoire 11 de l'équipement portable 1. Lors de la mise en œuvre du procédé, le module 3 est naturellement connecté à l'équipement mobile 1.

Le premier module 3 d'authentification comprend notamment une mémoire 31, un générateur de nombres aléatoires 32, un premier moyen de calcul 33, un deuxième moyen de calcul 34, un moyen de mémorisation 35 et un dispositif de commande 36.

La mémoire 31 mémorise des données DATA qui sont dans l'exemple des données nécessaires pour l'identification de l'équipement mobile 1 sur le réseau de communication 2, et une clé publique pkB de l'opérateur de communication 2.

Le générateur de nombres aléatoires 32 fournit sur demande du dispositif de commande une clé de transfert aléatoire RAND au premier moyen de calcul 33.

Le premier moyen de calcul 33 est adapté pour mettre en œuvre un procédé de chiffrement asymétrique tel qu'un procédé RSA (Rivest Shamir Adelman) ou un procédé basé sur des calculs sur courbes elliptiques. Il est utilisé pour chiffrer la clé RAND avec la clé publique pkB.

Le deuxième moyen de calcul 34 est adapté pour mettre en œuvre un procédé de chiffrement symétrique tel qu'un procédé DES (Data Encryption Standard) ou AES (Advanced Encryption Standard). Il est utilisé pour chiffrer les données DATA avec la clé RAND qu'il reçoit du générateur de nombres aléatoires.

Le moyen de mémorisation 35 est adapté pour mémoriser dans la mémoire 11 de l'équipement portable 1 la clé de transfert chiffrée $E_{pkB}(RAND)$ et les données chiffrées $E_{RAND}(DATA)$.

Le dispositif de commande 36 est adapté pour piloter le fonctionnement de la mémoire 31, du générateur de nombres aléatoires 32, du premier moyen de calcul 33, du deuxième moyen de calcul 34, et du moyen de mémorisation 35. Le

dispositif de commande est par exemple activé par l'utilisateur du premier module d'authentification.

Concrètement, dans l'exemple de la figure 3, le premier module d'authentification met en œuvre le procédé de dépôt selon la figure 1 de la manière suivante.

Dans une première étape, le dispositif de commande 36 du premier module 3 :

- active le générateur de nombres aléatoires 32 pour fournir une clé de transfert RAND
- active le premier moyen de calcul 33 qui chiffre la clé de transfert avec la clé publique pkB
- active le deuxième moyen de calcul 34 qui chiffre les données DATA contenues dans la mémoire 31 avec la clé de transfert RAND, puis
- active le moyen de mémorisation 35 qui mémorise la clé chiffrée $E_{RAND}(RAND)$ et les données chiffrées $E_{pkB}(RAND)$ dans la mémoire 11 de l'équipement mobile 1.

La figure 2 représente un organigramme général du procédé de récupération de données sécurisées selon l'invention.

Dans une première étape, le destinataire C récupère les données chiffrées $E_{RAND}(DATA)$ et la clé de transfert chiffrée $E_{pkB}(RAND)$ sur le support de stockage D.

Dans une deuxième étape, le destinataire C s'authentifie auprès du tiers de confiance B.

Dans une troisième étape, le destinataire C transmet au tiers de confiance la clé de transfert chiffrée.

Dans une quatrième étape et s'il a authentifié le destinataire C, le tiers déchiffre la clé de transfert chiffrée $E_{pkB}(RAND)$ avec sa clé privée et renvoie la clé de transfert RAND au destinataire C.

Dans une sixième étape, le destinataire C déchiffre les données chiffrées $E_{RAND}(DATA)$ avec la clé de transfert.

Dans l'exemple représenté sur la figure 3, le tiers de confiance B est l'opérateur de communication mobile 2, le destinataire C est un deuxième module 4 d'authentification d'utilisateur, et le support de stockage D est la mémoire 11 de l'équipement portable 1 dans lequel est connecté le deuxième module.

Le deuxième module 4 d'authentification comprend notamment un moyen de lecture 41, un moyen de communication 42, un troisième moyen de calcul 43, une mémoire 44 et un dispositif de commande 45.

Le moyen de lecture 41 est adapté pour lire dans la mémoire 11 les données chiffrées et la clé de transfert chiffrée.

Le moyen de communication 42 est adapté pour échanger des informations et / ou des données avec l'opérateur 2 de communication mobile, et notamment pour:

- transmettre à l'opérateur des données d'authentification personnelle,
- transmettre à l'opérateur la clé de transfert chiffrée,
- recevoir de l'opérateur la clé de transfert déchiffrée

Le troisième moyen de calcul 43 est adapté pour déchiffrer les données chiffrées $E_{RAND}(DATA)$ à l'aide de la clé de transfert fournie par l'opérateur. Les données DATA peuvent être ensuite par exemple mémorisées dans une mémoire 44 du deuxième module 4.

Le dispositif de commande 45 est adapté pour piloter le fonctionnement du moyen de lecture 41, du moyen de communication 42, du troisième moyen de calcul 43 et de la mémoire 44. Le dispositif de commande 45 est par exemple activé par le propriétaire du premier module d'authentification.

Concrètement, dans l'exemple de la figure 3, le procédé de récupération selon la figure 1 est mis en œuvre de la

manière suivante. Le deuxième module d'authentification 4 est connecté à l'équipement mobile 1 pour la mise en œuvre du procédé.

Dans la première étape, le dispositif de commande 45 active le moyen de lecture 41 qui va lire les données chiffrées et la clé de transfert chiffrée dans la mémoire 11.

Dans la deuxième étape, le dispositif de commande 45 active le moyen de communication 42, qui transmet à l'opérateur 2 des informations d'authentification du deuxième module 4.

Dans la troisième étape, le dispositif de commande 45 active le moyen de communication 42, qui transmet à l'opérateur 2 la clé de transfert chiffrée.

Dans la quatrième étape, l'opérateur 2 authentifie le deuxième module 4.

Dans la cinquième étape, si l'identité du deuxième module est correcte, l'opérateur déchiffre la clé de transfert avec sa clé privée personnelle, et renvoie la clé de transfert au deuxième module.

Dans la sixième étape, le dispositif de commande 45 active le troisième moyen de calcul qui déchiffre les données chiffrées $E_{RAND}(DATA)$ avec la clé de transfert.

De nombreuses variantes peuvent être apportées à l'exemple ci-dessus.

Dans l'exemple, le tiers de confiance est l'opérateur de communication mobile. Ce pourrait être n'importe quelle autre personne au sens large : personne physique ou morale, mais aussi serveur de données, etc. Il suffit que ladite personne dispose d'un jeu de clés comprenant une clé publique pkB et une clé privée associée, et de moyens matériels pour l'utiliser évidement.

Dans l'exemple encore, la clé publique pkB du tiers de confiance est mémorisée dans la mémoire 31 du premier module 3. La dite clé pourrait également être mémorisée dans la mémoire 11 de l'équipement mobile. Elle pourrait également être demandée par le module 3, au tiers de confiance par exemple ou à tout autre personne disposant de cette clé, juste avant son utilisation pour le chiffrement de la clé RAND.

Dans l'exemple encore, un procédé de chiffrement symétrique est utilisé pour chiffrer les données. Un procédé de chiffrement asymétrique pourrait également être utilisé, mais sa mise en œuvre serait plus lente et plus coûteuse que la mise en œuvre d'un procédé symétrique.

Dans l'exemple décrit, un procédé de chiffrement asymétrique est utilisé pour chiffrer la clé de transfert RAND. Ceci évite que le déposant et le destinataire ne se mettent préalablement d'accord sur une clé de transfert à utiliser. Par ailleurs, comme seul le chiffrement par la clé de transfert est utilisé dans les modules d'authentification, une implémentation non sécurisée de ce procédé de chiffrement est suffisante et peu coûteuse, et aisément réalisable sur une carte à puce. Le procédé de déchiffrement associé, bien plus coûteux est mis en œuvre par le tiers de confiance qui dispose de moyens matériels beaucoup plus conséquents tel qu'un serveur.

Dans l'exemple de la figure 3, le destinataire C transmet au tiers de confiance B des informations relatives à son identité que le tiers B vérifie pour authentifier ou non le destinataire C, c'est-à-dire pour valider ou non le droit d'accès aux données du destinataire C. On a supposé ainsi que le tiers B disposait préalablement d'informations suffisantes pour authentifier le destinataire C. Les informations d'authentification sont dans l'exemple des indications d'appartenance au réseau

de communication de l'opérateur tel qu'un numéro d'abonnement. Le déposant A peut ainsi dans l'exemple permettre l'utilisation de l'équipement mobile à toute personne disposant d'un module d'authentification au même réseau, sans préciser quelle personne explicitement.

Dans une variante, au cours du procédé de dépôt des données, le déposant A mémorise également sur le support de stockage des critères d'accès ID aux données comprenant notamment un haché de la clé RAND et des informations d'authentification du destinataire C. Ces critères d'accès prouvent que la clé RAND est associée aux données. Ces critères sont chiffrés avec la clé pkB et signés par le déposant. Au cours du procédé de récupération, le destinataire va transmettre au tiers de confiance les critères d'accès avec ses données d'authentification personnelles. Le tiers va alors utiliser ces critères ID et les données d'identification personnelles transmises par le destinataire pour l'authentifier.

Dans l'exemple enfin, le support de stockage D est la mémoire 11 de l'équipement mobile 1. De manière générale, le support de stockage est en quelque sorte un container, un moyen pour stocker des données numériques. Le support de stockage D peut par exemple être un support de mémorisation amovible, tel qu'un disque compact CD, un DVD (Digital Versatile Disc), une mémoire non volatile, un module mémoire, une carte SD (Secured Digital Card) ou tout autre type de carte mémoire. Il peut être conservé par une personne physique ou morale, et / ou être stocké dans un serveur de données.

L'exemple de la figure 3 montre une application de l'invention dans le domaine de la communication mobile. Bien d'autres applications sont envisageables. Plus précisément, toute application dans laquelle un déposant

souhaite transmettre de manière totalement sécurisée des données à un destinataire, éventuellement non identifié au moment du dépôt des données, et en limitant les contraintes imposées au tiers de confiance qui n'intervient plus qu'au moment de la récupération des données.

L'invention peut par exemple être utilisée pour la transmission d'informations au sein d'un groupe dynamique, dont les membres entrent et sortent à tout instant, les membres ne se connaissant pas nécessairement entre eux. Par exemple, les procédés selon l'invention peuvent être utilisés pour permettre à différents intervenants (personnes, entreprises) sur un site donné (une usine par exemple) de laisser des informations (par exemple liées à l'exploitation du site ou à l'intervention qui a été faite sur le site) à un ou plusieurs intervenants ultérieurs, les différents intervenants ne se connaissant pas nécessairement entre eux. Le tiers de confiance pourra être par exemple le propriétaire, le gestionnaire du site ou tout autre personne amenée à coordonner l'action des différents intervenants sur le site, sans toutefois avoir besoin ou intérêt à avoir connaissance des informations échangées entre les intervenants.

L'invention peut également avantageusement être utilisée pour toute application dans laquelle le déposant souhaite transmettre des informations tout en gardant un anonymat complet, ou dans laquelle le destinataire est anonyme pour le déposant.

A noter que l'existence du destinataire n'est pas nécessaire au moment du dépôt des données. De même, l'existence du déposant n'est plus nécessaire au moment du retrait des données.

REVENDICATIONS

1. Procédé de dépôt sécurisé de données (DATA), au cours duquel un déposant (A) chiffre les données (DATA) avec une clé de transfert (RAND) et chiffre la clé de transfert avec une clé d'un tiers de confiance (B), puis dépose les données chiffrées et la clé de transfert chiffrée sur un support de stockage (D).

2. Procédé selon la revendication 1, au cours duquel le déposant chiffre également des critères d'authentification (ID) d'un destinataire (C) des données chiffrées (E_{RAND}(DATA)) avec la clé (pkB) du tiers de confiance (B), puis mémorise les critères d'authentification chiffrés sur le support de stockage (D).

3. Procédé selon l'une des revendications 1 à 2, au cours duquel le déposant génère la clé de transfert (RAND) de manière aléatoire, avant de chiffrer les données (DATA) avec la clé de transfert (RAND).

4. Procédé selon l'une des revendications 1 à 3, au cours duquel le déposant chiffre les données par un procédé de chiffrement symétrique ou un procédé de chiffrement asymétrique.

5. Procédé selon l'une des revendications 1 à 4, au cours duquel le déposant chiffre la clé de transfert par un procédé de chiffrement asymétrique ou un procédé de chiffrement symétrique.

6. Procédé selon l'une des revendications 1 à 5, dans lequel le déposant (A) et / ou le tiers de confiance (B) sont :

- une ou des personne(s) physiques ou morales, ou
- un ou des module(s) d'authentification d'un abonné, ou
- un terminal ou des terminaux.

7. Procédé selon la revendication 6, dans lequel le déposant est un module d'authentification d'un abonné à un réseau de communication mobile et dans lequel le tiers de confiance est un opérateur exploitant ledit réseau de communication.

8. Procédé selon l'une des revendications 1 à 7, dans lequel le support de stockage (D) est :

- une mémoire (11) d'un terminal (1), tel qu'un téléphone portable, un ordinateur personnel ou un serveur, ou
- un support de mémorisation amovible tel qu'un disque compact, un DVD, une carte mémoire telle qu'une SD Card.

9. Procédé de récupération de données (DATA), au cours duquel :

- un destinataire (C) récupère sur un support de stockage (D) des données chiffrées ($E_{RAND}(DATA)$) avec une clé de transfert (RAND), et une clé de transfert chiffrée ($E_{pkB}(RAND)$) avec une clé d'un tiers de confiance (B),
- le destinataire s'authentifie auprès du tiers de confiance (B),
- le destinataire envoie la clé de transfert chiffrée au tiers de confiance,
- après authentification du destinataire (C), le tiers de confiance (B) déchiffre la clé de transfert chiffrée

(E_{pkB}(RAND)) avec sa clé et renvoie la clé de transfert (RAND) au destinataire (C),

- le destinataire déchiffre les données chiffrées (E_{RAND}(DATA)) avec la clé de transfert (RAND).

10. Procédé selon la revendication 9, dans lequel le tiers de confiance et / ou le destinataire sont:

- une ou des personne(s), ou
- un ou des module(s) d'authentification d'un abonné, ou
- un terminal ou des terminaux.

11. Procédé selon l'une des revendications 9 à 10, au cours duquel le destinataire déchiffre les données par un procédé de déchiffrement symétrique ou un procédé de déchiffrement asymétrique.

12. Procédé selon l'une des revendications 9 à 11, au cours duquel le tiers de confiance déchiffre la clé de transfert par un procédé de déchiffrement asymétrique ou un procédé de déchiffrement symétrique.

13. Dispositif de dépôt sécurisé de données, comprenant :

- un générateur de nombre aléatoire (32) pour générer une clé de transfert aléatoire (RAND),
- un premier moyen de calcul (33) pour chiffrer des données (DATA) avec la clé de transfert,
- un deuxième moyen de calcul (34) pour chiffrer la clé de transfert avec une clé d'un tiers de confiance (pkB), et
- un moyen (35) pour mémoriser les données chiffrées et la clé de transfert chiffrée sur un support de stockage (D, 11) accessible à un destinataire (C) des données.

14. Dispositif selon la revendication 13,

dans lequel le deuxième moyen de calcul (34) est également approprié pour chiffrer des critères d'authentification (ID) du destinataire (C) avec la clé du tiers de confiance (pkB), le module d'authentification comprenant également un moyen pour mémoriser les données d'authentification chiffrées sur le support de stockage.

15. Dispositif selon l'une des revendications 13 à 14, de type module d'authentification d'un abonné d'un réseau de communication.

16. Dispositif pour récupérer des données comprenant :

- un moyen de lecture (41), pour lire des données chiffrées (E_{RAND}(DATA) et une clé de transfert chiffrée (E_{pkB}(DATA)) sur un support de stockage (D),
- un moyen de communication (42) pour transmettre à un tiers de confiance des données d'authentification personnelles (ID) et la clé de transfert chiffrée, et pour recevoir du dit tiers la clé de transfert déchiffrée (RAND),
- un moyen de calcul (43) pour déchiffrer les données chiffrées avec la clé de transfert reçue du tiers de confiance.

17. Dispositif selon la revendication 16, de type module d'authentification (4) d'un abonné.

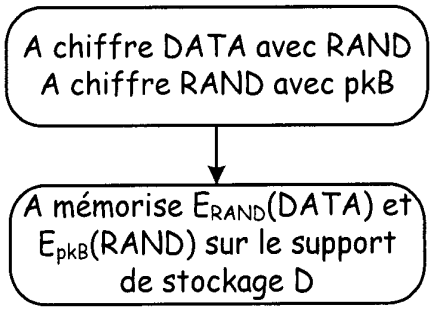
A chiffre DATA avec RAND
A chiffre RAND avec pkB
A mémorise E_{RAND}(DATA) et E_{pkB}(RAND) sur le support de stockage D

Fig. 1

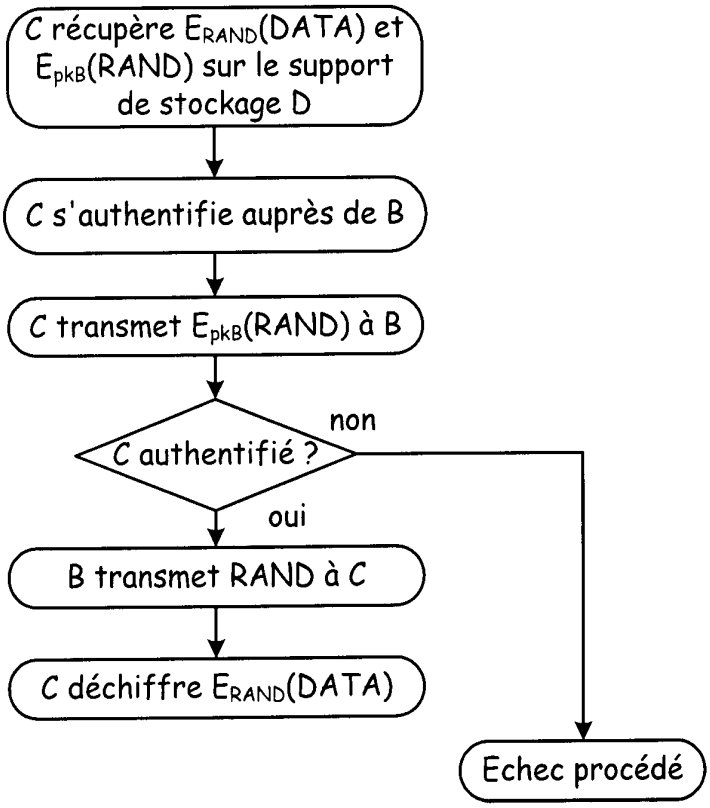
C récupère E_{RAND}(DATA) et E_{pkB}(RAND) sur le support de stockage D
C s'authentifie auprès de B
C transmet E_{pkB}(RAND) à B
C authentifié ?
non
oui
B transmet RAND à C
C déchiffre E_{RAND}(DATA)
Echec procédé

Fig. 2

2/2

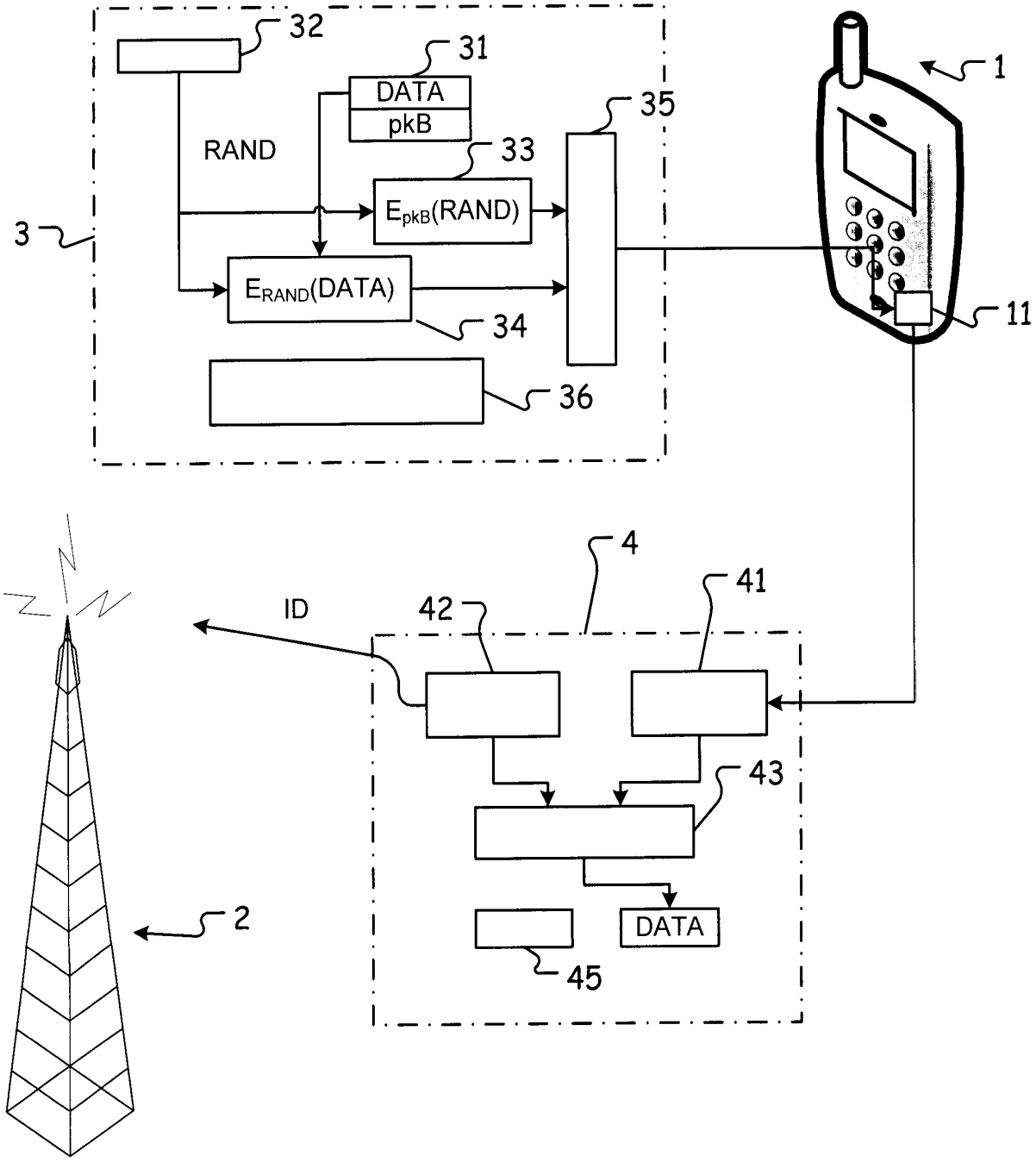
32
31
DATA
pkB
RAND
33
35
E_{pkB}(RAND)
3
E_{RAND}(DATA)
34
36
1
11
4
41
ID
42
43
2
DATA
45

Fig. 3

RÉPUBLIQUE FRANÇAISE

2892876

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 672341
FR 0511124

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 2005/091491 A1 (LEE LANE W ET AL) 28 avril 2005 (2005-04-28) * abrégé * * alinéa [0001] * * alinéa [0006] - alinéa [0010] * -----	1-17	H04L9/14
A	MENEZES, VANSTONE, OORSCHOT: "Handbook of applied Cryptography" 1997, CRC PRESS LLC , USA , XP002388064 * alinéa [0405] - alinéa [0407] * * alinéa [0491] * * alinéa [0547] - alinéa [0549] * * alinéa [0551] - alinéa [0554] * -----	1-17	
E	US 2005/257074 A1 (ALKOVE JAMES M ET AL) 17 novembre 2005 (2005-11-17) * abrégé * -----	1-17	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			G06F

Date d'achèvement de la recherche: 30 juin 2006

Examinateur: San Millán Maeso, J

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 0511124 FA 672341

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 30-06-2006
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 2005091491 A1	28-04-2005	AUCUN	
US 2005257074 A1	17-11-2005	AU 2005201847 A1	01-12-2005
		BR PI0501761 A	10-01-2006
		CA 2507369 A1	17-11-2005
		CN 1700193 A	23-11-2005
		EP 1598822 A2	23-11-2005
		JP 2005332399 A	02-12-2005

EPO FORM P0465