(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 974 208**

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

(21) **N° d'enregistrement national :** **11 01134**

(51) Int Cl[8] : ***G 06 K 17/00*** *(2012.01), G 06 Q 20/32, H 04 W 12/12*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 13.04.11.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 19.10.12 Bulletin 12/42.

(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) :** *PROTON WORLD INTERNATIONAL N.V.* — BE et *STMICROELECTRONICS (ROUSSET) SAS* — FR.

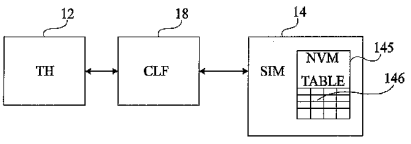
(72) **Inventeur(s) :** HUQUE THIERRY, VAN NIEUWENHUYZE OLIVIER et CHARLES ALEXANDRE.

(73) **Titulaire(s) :** PROTON WORLD INTERNATIONAL N.V., STMICROELECTRONICS (ROUSSET) SAS.

(74) **Mandataire(s) :** CABINET BEAUMONT.

(54) MECANISME DE CONTROLE D'ACCES POUR UN ELEMENT SECURISE COUPLE A UN CIRCUIT NFC.

(57) L'invention concerne un procédé de protection d'un module de sécurité (14) équipant un dispositif de télécommunication équipé d'un routeur (18) de communication en champ proche, contre une tentative de détournement d'un canal de communication entre un port de ce module de sécurité et un port du routeur, dans lequel à chaque requête provenant du routeur à destination du module de sécurité, ce dernier vérifie les droits d'accès aux informations qu'il contient en fonction de la provenance de la requête.



FR 2 974 208 - A1

MÉCANISME DE CONTRÔLE D'ACCÈS POUR UN ÉLÉMENT SÉCURISÉ COUPLÉ À UN CIRCUIT NFC

Domaine de l'invention

La présente invention concerne de façon générale les transactions effectuées au moyen de dispositifs mobiles de télécommunication de type téléphone portable. L'invention s'applique plus particulièrement à de tels dispositifs équipés en outre d'un circuit de communication en champ proche (NFC-Near Field Communication).

Exposé de l'art antérieur

De plus en plus, les téléphones mobiles sont équipés d'une interface de communication en champ proche qui leur permet de combiner des fonctions de transpondeurs électromagnétiques avec des fonctions de téléphonie mobile. En particulier, cela adjoint au dispositif mobile de télécommunication de type assistant personnel, téléphone mobile, Smartphone, etc., des fonctions d'émulation d'un transpondeur électromagnétique, de type carte sans contact ou lecteur de carte sans contact. Cela enrichit considérablement les fonctionnalités du dispositif mobile qui peut alors servir, par exemple, de porte-monnaie électronique, de dispositif de validation d'accès, de titre de transport, etc.

Pour émuler le fonctionnement d'une carte à puce sans contact, le dispositif mobile de télécommunication est équipé d'un circuit intégré d'émission-réception en champ proche (CLF-Contact Less Front End) également appelé routeur NFC. Ce routeur est équipé d'une tête d'émission-réception radiofréquence (RF) associée à une antenne de faible portée pour communiquer à la manière d'un transpondeur électromagnétique. Le routeur exploite les capacités du ou des processeurs de traitement du dispositif mobile pour les opérations de traitement et de mémorisation des données. Pour des applications de contrôle d'accès, de porte-monnaie électronique, de paiement, etc., on exploite un élément sécurisé permettant d'authentifier l'utilisateur. Cet élément sécurisé est soit intégré au dispositif mobile de télécommunication (circuit intégré dédié, circuit soudé à la carte de circuit imprimé), soit contenu dans un microcircuit porté par un module d'identification d'abonné (SIM-Subscriber Identification Module), ou tout autre carte amovible, par exemple, au format standard d'une carte mémoire).

Un routeur NFC peut également être présent dans un dispositif mobile de type clé USB, dans un terminal de paiement bancaire, dans un dispositif adhésif (sticker), etc.

Une émulation d'une carte sans contact dans un dispositif mobile de télécommunication est susceptible d'engendrer des faiblesses du point de vue de la sécurité des transactions.

Il serait souhaitable d'éviter ces faiblesses afin de sécuriser les transactions.

Résumé

Un objet d'un mode de réalisation de la présente invention est de pallier tout ou partie des inconvénients des dispositifs mobiles de télécommunication associés à un module de transmission en champ proche.

Un autre objet d'un mode de réalisation de la présente invention est d'améliorer la sécurité contre une tentative de piratage d'un module de sécurité de type module d'identification

d'abonné, contenu dans un dispositif de télécommunication associé à un module de transmission en champ proche.

Pour atteindre tout ou partie de ces objets ainsi que d'autres, un mode de réalisation de la présente invention prévoit un procédé de protection d'un module de sécurité équipant un dispositif de télécommunication équipé d'un routeur de communication en champ proche, contre une tentative de détournement d'un canal de communication entre un port de ce module de sécurité et un port du routeur, dans lequel à chaque requête provenant du routeur à destination du module de sécurité, ce dernier vérifie les droits d'accès aux informations qu'il contient en fonction de la provenance de la requête.

Selon un mode de réalisation de la présente invention, le module de sécurité n'autorise une transaction que si la requête provient d'une communication en champ proche.

On prévoit également un module de sécurité destiné à un dispositif de télécommunication équipé d'un routeur de communication en champ proche, comportant une mémoire non volatile de stockage des droits d'accès conformément au procédé ci-dessus.

Selon un mode de réalisation de la présente invention, ladite mémoire contient une table contenant, pour chaque requête susceptible d'être reçue, un identifiant de port du routeur et un identifiant de la source logique d'où émane la requête.

Selon un mode de réalisation de la présente invention, le droit d'accès est conditionné par la source logique.

On prévoit également un dispositif de télécommunication équipé d'un routeur de communication en champ proche et d'un module de sécurité.

Brève description des dessins

Ces objets, caractéristiques et avantages, ainsi que d'autres seront exposés en détail dans la description suivante de modes de réalisation particuliers faite à titre non-limitatif en relation avec les figures jointes parmi lesquelles :

la figure 1 représente schématiquement un dispositif mobile de télécommunication du type auquel s'applique à titre d'exemple la présente invention ;

la figure 2 est un schéma illustrant une fonction d'un module de transmission en champ proche du dispositif de la figure 1 ;

la figure 3 illustre de façon très schématique, une attaque susceptible d'exploiter une faiblesse du dispositif de télécommunication de la figure 1 ;

la figure 4 illustre un exemple de déroulement d'une attaque appliquée à la norme de paiement EMV ;

la figure 5 illustre un mode de mise en oeuvre d'une phase préparatoire à une telle attaque ;

la figure 6 est un schéma bloc simplifié d'un mode de réalisation d'un mécanisme de protection contre une attaque du type de celle illustrée en figures 3 et 5 ;

la figure 7 illustre sous la forme d'une table, un mode de réalisation de la présente invention ;

la figure 8 illustre, de façon très schématique, un mode de mise en oeuvre du mécanisme de protection ; et

la figure 9 illustre, de façon très schématique, un mode de configuration d'un module de sécurité pour la mise en oeuvre de l'invention.

Description détaillée

De mêmes éléments ont été désignés par des mêmes références aux différentes figures. Par souci de clarté, seuls les éléments et étapes utiles à la compréhension de l'invention ont été représentés et seront décrits. En particulier, les protocoles de codage et de communication, que ce soit pour les transmissions en champ proche ou pour les télécommunications en mode GSM, n'ont pas été détaillés, l'invention étant compatible avec les protocoles usuels. De plus, les circuits constitutifs du dispositif mobile de communication n'ont pas non plus été détaillés, l'invention étant là encore compatible avec les dispositifs usuels, pourvu que ceux-ci soient programmables.

La figure 1 représente, de façon très schématique, un dispositif mobile de télécommunication (par exemple un téléphone portable) du type auquel s'applique à titre d'exemple la présente invention. Les différents éléments d'interface avec l'utilisateur (clavier, écran, haut-parleurs, etc.) n'ont pas été représentés, ces éléments n'étant pas modifiés par la mise en oeuvre des modes de réalisation qui vont être décrits.

Le dispositif 1 comporte une unité centrale de traitement 12 (CPU/TH) qui est constituée d'au moins un microcontrôleur formant le coeur du dispositif. Ce microcontrôleur est couramment désigné par son appellation anglo-saxonne "terminal host". Pour le fonctionnement en télécommunication par l'intermédiaire d'un réseau (GSM, 3G, UMTS, etc.), ce microcontrôleur exploite des informations d'identification et d'authentification fournies par un module d'identification d'abonné 14 (SIM) qui constitue un module de sécurité du dispositif. Le microcontrôleur 12 est susceptible d'exploiter une ou plusieurs mémoires internes non représentées du téléphone. Le téléphone 1 peut également comporter un lecteur 16 de carte mémoire ou autres bus de communication avec l'extérieur pour charger, dans le téléphone, des données et/ou des applications.

Les dispositifs mobiles auxquels s'appliquent les modes de réalisation décrits combinent la fonction de télécommunication avec celle d'un système de transmission sans contact en champ proche (NFC). Pour cela, le dispositif 1 comporte un circuit 18 (CLF) constituant un module de communication en champ proche à la manière d'un transpondeur électromagnétique. Ce module 18, également appelé routeur NFC, est associé à une antenne 182 distincte d'une antenne 20 destinée au réseau de téléphonie mobile. Le cas échéant, le circuit 18 est associé à un module de sécurité (SSE) 24 distinct de la carte SIM 14 et directement présent sur la carte de circuit imprimé du téléphone, ou porté par une carte amovible à microcircuit (par exemple, au format d'une carte mémoire). Un

module de sécurité est un circuit électronique d'exécution des applications de manière sécurisée, garantissant la sécurité (secret/intégrité) de données manipulées par ces applications.

Les différents éléments du dispositif 1 communiquent selon différents protocoles. Par exemple, les circuits 12 et 18 communiquent par une liaison 1218 de type I2C (ou SPI), la carte SIM 14 communique avec le microcontrôleur 12 par une liaison 1214 conforme à la norme ISO 7816-3, de même que le module de sécurité 24 communique avec le routeur 18 selon cette norme par une liaison 2418. Le routeur 18 communique avec la carte SIM par exemple par un bus unifilaire 1418 (SWP - Single Wire Protocol). D'autres versions de protocoles et de liaisons sont bien entendu possibles.

Les modes de réalisation seront décrits en relation avec un téléphone GSM. L'invention s'applique toutefois plus généralement à tout dispositif de télécommunication adapté à un réseau mobile (par exemple, de type Wifi, Bluetooth, WiMax, etc.) et associé à un module de transmission sans contact (routeur NFC), par exemple, une clé USB, un terminal bancaire, un compteur de consommation d'énergie ou autres, un terminal de validation d'accès, de titres de transport, etc.

De même, on désignera par le terme routeur le module de communication en champ proche, car celui-ci intègre généralement, dans un même circuit, toutes les fonctions utiles à l'émulation d'une carte sans contact mais les modes de réalisation décrits s'appliquent à tout type de module NFC.

Le routeur 18 comporte des bornes physiques (TERMINALS) de raccordement des liaisons 1218, 1418 et 2418 et gère des ports logiques (GATES) d'affectation de ces bornes aux différentes fonctions liées aux communications en champ proche. Le routeur 18 inclut donc un processeur et des mémoires volatiles et non volatiles pour stocker, entre autres, une table de routage des différents ports logiques. Certains ports sont réservés à des fonctions d'administration du routeur et d'autres sont d'affectation libre par le routeur.

En fonctionnement, le routeur 18 met à disposition et gère différents canaux de communication avec les autres circuits 12, 14, 24, etc. du dispositif mobile pour leur donner accès aux fonctions de communication en champ proche, c'est-à-dire à des ports connectés à des circuits de transmission radiofréquence, désignés ports radiofréquence ou RF.

La figure 2 illustre, de façon très schématique et sous forme de blocs, la fonction routage du routeur 18. Pour simplifier, la figure 2 est une représentation structurelle alors qu'en pratique l'affectation des différents ports aux différents circuits du dispositif mobile est effectuée de façon logicielle par la table de routage.

Chacune des bornes (TERMINALS) du routeur se voit affecter un ou plusieurs ports (GATES). Dans l'exemple de la figure 2, on suppose que les liaisons physiques 1418 et 1218 de la carte SIM 14 et du microcontrôleur 12 sont connectées à des bornes du routeur 18 et que des ports (GATES) sont affectés à ces circuits. Plusieurs ports peuvent être affectés à un même circuit (ce qui est symbolisé en figure 2 par la connexion d'une même borne à plusieurs ports). La table de routage (ROUTING TABLE) du routeur 18 affecte certains ports à des fonctions internes (par exemple de configuration et d'administration), mais également ouvre des canaux (PIPE) entre certains ports affectés à la carte SIM ou au microcontrôleur RF, et des ports (RFGATES) inclus dans le module 18. Cela correspond à l'ouverture de canaux (PIPE) entre les circuits externes aux routeurs 18 et ces circuits de transmission RF pour la mise en oeuvre des différentes applications requérant une communication en champ proche. Par exemple, dans les applications bancaires, de transports, de porte-monnaies électroniques, d'accès, etc. requérant une identification ou authentification sécurisée de l'utilisateur, un ou plusieurs canaux sont ouverts entre le routeur et la carte SIM pour exploiter les informations sécurisées d'identification de l'utilisateur et valider la transaction.

L'intégration de routeurs NFC dans des dispositifs mobiles de télécommunication et le partage d'un même module de sécurité (carte SIM ou autre) engendre certaines faiblesses du point de vue de la sécurité.

On pourrait prévoir des outils d'authentification pour s'assurer que les liaisons entre le routeur et les différents circuits externes ne sont pas piratés. Toutefois, cela s'avère insuffisant face à une faiblesse que les inventeurs ont identifiée et qui sera décrite ci-après.

Le routeur 18 ou module NFC est généralement un seul circuit intégré et ses accès externes sont plutôt bien protégés contre d'éventuelles tentatives de piratage.

Jusqu'à présent, on s'est surtout préoccupé de garantir qu'une transaction en champ proche émulée par le dispositif mobile ne permette pas à un dispositif pirate interceptant la communication en champ proche d'exploiter les informations fournies par le module de sécurité.

Toutefois, un risque reste présent car le routeur 18 gère également un canal (ATPIPE) symbolisé en pointillé en figure 2) de communication entre la carte SIM 14 (ou tout autre module de sécurité) et le microcontrôleur 12 du dispositif mobile de télécommunication. Ce canal est normalement utilisé pour que la carte SIM 14 informe le microcontrôleur 12 qu'un message lui parvient par la liaison NFC. Toutefois, il est également possible de détourner cette utilisation pour faire croire au module de sécurité 14 qu'il communique avec le routeur pour une transaction en champ proche, donc sur un canal avec les ports RF du téléphone, alors qu'il en fait en communication avec le microcontrôleur 12.

La figure 3 illustre, de façon très schématique et sous forme de blocs, l'exploitation possible d'un canal ATPIPE entre une carte SIM 14 et un microcontrôleur 12 d'un téléphone mobile 1.

On suppose que, dans une phase préparatoire à l'attaque, le téléphone GSM 1 a été piraté et qu'un canal ATPIPE

a été détourné par l'intermédiaire du routeur 18 entre sa carte SIM 14 et son microcontrôleur 12. La table de routage du routeur 18 contient donc l'information de ce canal "dérouté". On suppose également qu'une application pirate (PA) a été stockée dans une mémoire 13 (non volatile) du téléphone 1 et que cette application peut donner des instructions au microcontrôleur 12. Plusieurs modes de mise en oeuvre de la phase préparatoire seront exposés ultérieurement.

L'utilisateur du dispositif 1, une fois celui-ci piraté par le chargement de l'application PA et par l'ouverture du canal ATPIPE, n'est pas en mesure, comme le verra par la suite, de s'apercevoir d'un dysfonctionnement. Il utilise son téléphone de façon normale.

L'une des fonctions de l'application PA est de déclencher automatiquement une réponse du téléphone 1 suite à une requête provenant du réseau de télécommunication et émise par un autre dispositif mobile 3 en possession de l'attaquant. Le dispositif pirate est, par exemple, un autre téléphone GSM 3 qui utilise son propre module d'identification d'abonné pour communiquer via le réseau GSM (symbolisé par une antenne relais 5). Il peut s'agir également d'un microordinateur associé à un modem GSM.

Dans l'exemple de la figure 3, le dispositif 3 est également équipé d'un routeur sans contact, par exemple pour initier des transactions en champ proche avec une borne 7 (par exemple, un terminal NFC ou tout autre borne de communication sans contact - CONTACT LESS TERMINAL). Par exemple, le dispositif 3 est utilisé pour réaliser un achat avec un paiement devant être validé par son routeur NFC.

Normalement, pour un tel paiement, le routeur du téléphone 3 gère un canal de communication avec le module d'identification d'abonné (ou tout autre module de sécurité dédié) de ce téléphone pour authentifier l'utilisateur et valider le paiement.

La figure 4 illustre un exemple d'échange au moment de la validation du paiement dans un mécanisme tel qu'illustré en figure 3.

Le téléphone 3 ou dispositif pirate PR reçoit, de son module NFC, une demande de validation de paiement. Une telle demande est, par exemple, supportée par une application selon la norme EMV (Eurocard-Mastercard-Visa). Le routeur NFC du téléphone 3 reçoit donc une instruction de sélection de son application EMV (SELECT EMV). Au lieu d'utiliser son propre module de sécurité, le téléphone 3 utilise le réseau GSM 5 pour demander au téléphone distant 1 de valider le paiement au moyen du module d'identification d'abonné 14. Par exemple, le dispositif 3 envoie un SMS par l'intermédiaire du réseau 5 qui, lorsqu'il est reçu par le téléphone 1, est traité par l'application pirate. Ce SMS contient, par exemple, une instruction de sélection de l'application EMV (SELECT EMV). Côté téléphone 1, l'application pirate simule les requêtes provenant du port RF et utilise le microcontrôleur 12 pour transmettre ces requêtes au routeur 18 (CLF) qui les fait suivre par le canal ATPIPE au module d'identification 14 (SIM). Ce dernier reçoit donc l'instruction SELECT EMV et valide la sélection de l'application EMV. Cette validation est détournée par l'application pirate exécutée sur microcontrôleur 12 et renvoyée au dispositif 3. L'obtention, par le dispositif pirate, de la validation de l'application EMV du module de sécurité 18 du dispositif 1 est exploitée par son routeur NFC pour communiquer avec le terminal de paiement 7. Toute la transaction de paiement est véhiculée par ce canal piraté jusqu'à la validation (OK) du paiement par la carte SIM du téléphone 1 transmise par le réseau GSM puis par le téléphone 3 jusqu'au terminal 7. Il en découle que le paiement est débité à l'abonné du téléphone 1 et non à l'attaquant possédant le dispositif 3. Le plus souvent, une application sans contact ne requiert aucune interaction avec le terminal (7, figure 3) à l'exception d'une présentation du dispositif sans contact. En particulier, aucune saisie de code

(PIN) n'est nécessaire pour une transaction en champ proche afin de ne pas rallonger la durée de la transaction, de sorte que le dispositif 3 peut pirater sans difficultés le dispositif distant 1.

Les contre-mesures prévoyant des chiffrements et/ou des signatures entre la borne 7 réclamant l'authentification et le module de sécurité sont inefficaces pour contrer cette attaque. En effet, les informations entre la borne 7 et le module 14 n'ont pas besoin d'être décodées. On a en fait établi un canal de communication entre le module 14 du téléphone 1 et la borne 7 via le réseau de télécommunication 5, de sorte que le module 14 se comporte comme s'il était en transaction en champ proche avec la borne 7.

Le même type de piratage peut intervenir pour des applications d'authentification ou de validation de passage, de type accès sécurisé.

De plus, cette attaque peut également prospérer même sans que le dispositif pirate 3 utilise son propre routeur NFC, mais par exemple utilise un mode de communication à contact, pourvu que l'authentification réclamée provienne d'un module de sécurité et respecte les formats et protocoles utilisés par le protocole NFC. Par ailleurs, une telle attaque peut servir à détourner n'importe quelle information du dispositif 1 au profit d'un système pirate (par exemple, les données dupliquant le contenu de la piste magnétique d'une carte dans une application au paiement bancaire).

En outre, l'attaque peut faire intervenir la carte SIM du téléphone 1, ou tout autre module de sécurité (par exemple, le module 24, figure 1), pourvu que le canal soit géré par le routeur 18 entre ce module et un circuit (généralement le microcontrôleur 12) capable de gérer les communications sur le réseau 5.

Cette attaque de transaction en champ proche, exploitant le réseau de télécommunication, est due à la présence

d'un canal de communication, via le routeur NFC, entre le module de sécurité et un microcontrôleur connecté à ce routeur.

La mise en oeuvre de l'attaque requiert une phase préparatoire dans laquelle il faut intervenir sur le téléphone 1 que l'on souhaite pirater.

Cette préparation requiert une intervention plus ou moins importante selon le niveau de sécurité apportée par la carte SIM à la gestion des canaux de communication NFC.

Dans un mode de réalisation simplifié, le microcontrôleur est autorisé à créer un canal sur n'importe quel port libre. Dans ce cas, une application pirate, chargée dans le microcontrôleur, est susceptible d'ouvrir un canal à travers le routeur NFC jusqu'à la carte SIM. Si, par la suite, la carte SIM n'effectue pas d'autres vérifications que de constater que le format des requêtes correspond à un format de trame radiofréquence émanant d'un circuit NFC, l'application pirate peut attaquer la carte SIM.

Selon un autre mode de réalisation, le module de sécurité 14 est plus évolué et vérifie l'association entre les numéros de canaux ou de ses propres ports et les ports RF.

Dans le premier cas, on considère que la carte SIM 14 ne tient pas compte du circuit avec lequel le port est ouvert (donc qu'il peut s'agir d'un port destiné au microcontrôleur). Ce code de mise en oeuvre exploite le fait que l'attribution des numéros (identifiants) de canaux est souvent séquentielle. On commence alors par demander au microcontrôleur de supprimer un canal entre la carte SIM et les ports RF. Puis, on propose la création et l'ouverture d'un canal ayant le même identifiant entre le microcontrôleur et la carte SIM.

La figure 5 illustre un autre mode de mise en oeuvre d'une phase préparatoire de l'attaque visant à détourner un canal entre le routeur 18 (CLF) et la carte SIM (SIM1) d'un utilisateur. Ce mode de mise en oeuvre est plus particulièrement destiné au second exemple ci-dessus où la carte SIM s'assure, avant de transmettre des informations vers le routeur CLF,

qu'elle a bien contrôlé l'ouverture du canal de communication avec celui-ci. On exploite ici le fait que, préalablement à l'initialisation du dispositif 1, la carte SIM vérifie si elle s'est déjà trouvée en présence du routeur 18. Si ce n'est pas le cas, elle reconfigure les canaux entre ses ports et le routeur NFC.

Dans un fonctionnement normal, lors d'une première connexion de la carte SIM1 dans le téléphone 1, la carte provoque l'ouverture, au niveau d'une couche dite de transport, d'au moins un canal de communication, identifié SYNCID1, avec le routeur CLF. Pour cela, la carte SIM1 envoie au routeur CLF à la fois une donnée SYNCID1 de synchronisation et un nombre quelconque (typiquement un nombre aléatoire RD1). Le nombre RD1 est stocké dans le routeur CLF et sert à la carte 14 pour vérifier qu'elle a déjà provoquée une ouverture de canal avec ce routeur. A chaque initialisation, la carte vérifie l'existence du numéro RD1 dans le routeur. Au niveau applicatif, la carte demande au routeur l'ouverture d'un canal entre un de ses ports, identifié GATEID et l'un des ports RF, identifié RFGATEID. Le routeur ouvre alors un canal et lui attribue un identifiant PIPEID et, à la fois, le stocke dans la table de routage et le communique à la carte SIM1. A chaque fois qu'une donnée est demandée par le routeur, la carte SIM1 vérifie que l'identifiant PIPEID du canal est correcte.

Pour mettre en place l'attaque, le pirate doit disposer pendant un laps de temps du téléphone mobile 1 et de la carte SIM1. Cela est relativement facile, par exemple, en se faisant prêter le téléphone mobile pour soi-disant passer un appel, ou en utilisant frauduleusement un téléphone lors d'une intervention de maintenance, par exemple dans un magasin de téléphonie mobile.

Avec la carte SIM1 et le téléphone muni du routeur 1, le fraudeur commence par introduire la carte SIM1 dans un dispositif pirate (pirate READER), par exemple un autre téléphone mobile dont le microcontrôleur est capable d'exécuter

un programme de piratage respectant les fonctions décrites, ou un ordinateur équipé d'un lecteur de carte et qui simule un routeur. La carte SIM1 n'ayant jamais rencontré le routeur NFC du dispositif pirate ou un routeur émulé par ce dispositif, elle génère un nouvel identifiant de synchronisation SYNCID2. Elle renvoie des identifiants de port RFGATEID et GATEID pour l'ouverture des canaux correspondants. Le routeur pirate attribue alors, à au moins une paire de ports, un canal FPIPEID qui correspond à une passerelle entre le routeur et un port externe du microcontrôleur, au lieu d'associer le port GATEID à un port RF. L'identifiant FPIPEID est alors chargé dans une carte SIM2 falsifiée ainsi que les identifiants RSYNCHID2 et RD2. La carte SIM2 contient alors une table de routage associant, au canal FPIPEID, les ports RFGATEID et GATEID.

Puis, cette carte SIM2 est introduite dans le téléphone 1. Les identifiants SYNCID2 et RD2 sont alors transférés au routeur CLF 18 pour l'ouverture du canal FPIPEID entre des ports désignés GATEID et RFID. Cela revient à modifier la table de routage du routeur pour que, lorsque le canal entre les ports GATEID et RFGATEID est appelé, le canal affecté soit le canal FPIPEID au lieu de PIPEID.

L'attribution du canal FPIDEID peut comprendre diverses formes en fonction de la façon avec laquelle les canaux sont attribués aux ports dans le routeur. Par exemple, on passe par une phase d'observation de l'affectation des canaux en plaçant la carte SIM2 dans le routeur pour observer la méthode d'affectation des canaux, avant d'introduire cette carte SIM2 dans le lecteur pirate.

On replace enfin la "vraie" carte SIM1 dans le téléphone 1. Comme le routeur CLF connaît les identifiants RD2 et SYNCID2, la carte considère "connaître" le routeur et ne provoque pas la réouverture de canaux avec celui-ci. Lorsque la carte SIM1 demande une communication vers le port RFGATEID, le routeur utilise le canal FPIPEID qui a été attribué.

Le terminal GSM a bien été piraté, c'est-à-dire qu'un canal FPIPE (ou ATPIPE, figure 2) a été ouvert entre un port GATEID de la carte SIM et un port du microcontrôleur 12, alors que la carte SIM1 croît que ce canal relie son port GATEID au port RFGATEID. Ce canal peut alors être détourné pour un accès à distance par le réseau GSM depuis un autre terminal (figure 3). Le téléchargement de l'application pirate PA peut s'effectuer soit ultérieurement, soit en même temps que la génération du canal pirate.

Diverses possibilités existent en fonction du dispositif 1 en présence pour avoir accès à sa table de routage. Par exemple, on peut lire la table de routage. Si cela n'est pas possible, on peut lors du passage de la carte SIM1 dans le lecteur pirate, émuler un fonctionnement de circuit CLF, afin d'obtenir la configuration complète stockée dans cette carte. On peut également utiliser une carte pirate SYNC2 ou un émulateur de carte pour, dans le téléphone VALID1, extraire les informations de la table de routage.

On voit donc qu'il est possible de paramétrer un détournement d'un canal de communication entre un module de sécurité et un routeur NFC pour établir un canal entre ce module et le microcontrôleur du téléphone, externe au routeur NFC.

Pour que l'utilisateur du téléphone 1 ne s'aperçoive pas du piratage, même lorsqu'il utilise son mode sans contact, l'application pirate doit comporter la fonction de rediriger le canal FPIPE vers les circuits RF du routeur lorsqu'une requête d'information vers la carte SIM est émise par le routeur 18.

La figure 6 représente, partiellement et sous forme de blocs, des éléments d'un dispositif mobile de télécommunication selon un mode de réalisation d'un mécanisme de protection contre le type d'attaque décrit ci-dessus.

Comme en figure 1, on retrouve une unité centrale de traitement 12 (TH - Terminal Host) susceptible de communiquer avec un routeur sans contact 18 (CLF), lui-même capable d'échanger avec un module de sécurité 14 (par exemple une carte

SIM). De façon usuelle, le routeur 18 comporte une table de routage (non représentée) mettant en correspondance un identifiant de canal PIPEID avec deux identifiants de ports GATEID entre lesquels le canal est ouvert.

Selon le mode de réalisation de la figure 6, le module de sécurité 14 inclut une table de filtrage contenant, pour chaque fonction requérant un traitement par la SIM et dont une requête est envoyée par le routeur 18, des paramètres permettant au module de sécurité de déterminer si cette fonction doit être autorisée ou non. Ainsi, le module de sécurité est modifié pour contenir, dans une mémoire non volatile 145 (NVM) qu'il contient, une table 146 déterminant, à partir d'une fonction appelée par le routeur 18, si la transaction doit ou non être autorisée.

La figure 7 illustre un mode de réalisation simplifié d'une table 146 stockée en mémoire non volatile (145, figure 6) d'un module de sécurité. Cette table stocke en regard d'un identifiant de l'application ou de la fonction APPLI appelée par le routeur 18 et de la provenance de la requête (Log Source ID), le droit (Y) ou non (N) d'accès à la carte SIM. En fonction de ce droit (right), la carte SIM répond que la fonction est ou non accessible. Un exemple plus détaillé de table sera illustré ultérieurement.

La figure 8 illustre un mode de mise en oeuvre du mécanisme de sécurisation, basé sur l'utilisation d'une table telle qu'illustrée par la figure 7.

A chaque fois qu'une source logique cherche à utiliser le routeur 18 (CLF) pour transmettre une demande d'accès à une application i (APPLIi) du module de sécurité 14 (SIM), elle envoie une requête de sélection SELECT à la carte SIM qui transite par le routeur. La carte SIM vérifie (CHECK), dans la table stockée dans sa mémoire non volatile (NVM), si les droits sont accordés à cette application.

Dans la partie haute de la figure 8, on suppose que l'accès est autorisé. Le microcontrôleur de la carte SIM lit le

résultat de la mémoire non volatile (OK) et transmet à la source logique via le routeur 18 une acceptation de la requête de sélection de cette application. La transaction peut alors s'opérer entre la source logique et la carte SIM.

Dans la partie basse de la figure 8, on suppose que la table retourne une absence de droit (NO) à l'application sélectionnée. La carte SIM renvoie alors un message d'erreur (ERROR) au routeur comme quoi l'application n'est pas présente ou n'est pas disponible dans la carte (APPLIi NOT FOUND).

La figure 9 illustre un mode de réalisation d'une étape d'initialisation de la carte SIM pour la mise en oeuvre du procédé décrit plus haut.

Le fournisseur (Issuer) de la carte SIM doit mémoriser, dans la mémoire non volatile NVM, les droits des différentes applications. Pour cela, chaque instance d'application (code de l'application plus jeu de paramètres nécessaire à son exécution) est installé dans la carte SIM (INSTALL APPLIi) qui provoque l'écriture des droits correspondants dans la table (WRITE TABLE) et envoie un accusé réception ACK en retour au dispositif d'installation. Ce dispositif est en général un terminal de personnalisation de la carte SIM et plus généralement tout système utilisé pour paramétrer ou personnaliser un module de sécurité, incluant également les systèmes de mise à jour usuels des dispositifs mobiles (mises à jour communément appelées "over the air").

Les tableaux ci-dessous illustrent un exemple plus complet de contenu d'une table dans un module de sécurité selon un autre mode de réalisation.

Cet exemple s'applique plus particulièrement à un routeur NFC compatible avec la norme ETSI. Dans cette norme, chaque canal (PIPE) connecte deux ports (GATE) appartenant chacun à un circuit (HOST) connectant au moins un port. Chaque canal connecté au module de sécurité peut être caractérisé par trois informations : l'identifiant du canal (PIPE ID), l'identifiant du circuit (Ext Host ID) et l'identifiant du port

destinataire. Ces informations sont stockées dans le routeur CLF. On prévoit de les stocker dans le module de sécurité en les complétant par l'information de la source logique Logical Source ID.

Le tableau I ci-dessous donne en colonne de droite une description de la source logique correspondante.

TABLEAU I

PIPE ID	Ext Host ID	Ext Gate ID	LOGICAL SOURCE ID	Logical Source Description
00	00 (CLF)	--	00	CLF - Gestion des ports
01	00 (CLF)	--	00	CLF - port d'administration
02	00 (CLF)	01	00	CLF - canal propriétaire
03	00 (CLF)	21	01	Emulation Carte RF - Type B
04	00 (CLF)	23	01	Emulation Carte RF - Type A
05	00 (CLF)	24	01	Emulation Carte RF - Type C
06	00 (CLF)	11	02	Lecteur RF - Type B
07	00 (CLF)	13	02	Lecteur RF - Type A
08	00 (CLF)	04	00	CLF - Echo
09	00 (CLF)	05	00	CLF - Gestion d'identité
0A	01 (TH)	33	04	SE Connexion directe
0B	01 (TH)	41	05	TH - Connectivité
0C	01 (TH)	04	03	TH - Echo
0D	01 (TH)	05	03	TH - Gestion d'identité

Les droits d'accès sont conditionnés par l'identifiant de la source logique.

Des exemples d'identifiants de source logique sont donnés dans le tableau II reproduit ci-dessous :

TABLEAU II

Logical Source ID	Description de source Logique
00	Ports d'administration du CLF
01	Emulation RF de la carte
02	Lecteur RF
03	Ports d'administration de l'Hôte TH
04	Connexion directe vers le module de sécurité
05	Connexion selon la norme ETSI 102622

Ce tableau sert à définir le droit d'accès au module de sécurité comme illustré par la figure 7.

La mise en oeuvre des modes de réalisation décrits ne requiert aucune modification du routeur CLF. Seul le module de sécurité est concerné. Par conséquent, la mise en oeuvre de ces modes de réalisation est compatible avec les dispositifs existants.

Divers modes de réalisation ont été décrits, diverses variantes et modifications apparaîtront à l'homme de l'art. En particulier, les modes de réalisation ont été décrits en relation avec un exemple de module de sécurité constitué d'une carte SIM. Il s'applique toutefois plus généralement à tout module de sécurité susceptible de communiquer avec un routeur NFC. De plus, la mise pratique de l'invention est à la portée de l'homme du métier en utilisant des outils de programmation en eux-mêmes usuels.

REVENDICATIONS

1. Procédé de protection d'un module de sécurité (14) équipant un dispositif de télécommunication (1) équipé d'un routeur (18) de communication en champ proche, contre une tentative de détournement d'un canal de communication entre un port (GATES) de ce module de sécurité et un port (RFGATE) du routeur, dans lequel à chaque requête provenant du routeur à destination du module de sécurité, ce dernier vérifie les droits d'accès aux informations qu'il contient en fonction de la provenance de la requête.

2. Procédé selon la revendication 1, dans lequel le module de sécurité (14) n'autorise une transaction que si la requête provient d'une communication en champ proche.

3. Module de sécurité (14) destiné à un dispositif de télécommunication équipé d'un routeur (18) de communication en champ proche, comportant une mémoire non volatile (145) de stockage des droits d'accès conformément au procédé selon la revendication 1 ou 2.

4. Module selon la revendication 3, dans lequel ladite mémoire (145) contient une table (146) contenant, pour chaque requête susceptible d'être reçue, un identifiant de port du routeur et un identifiant de la source logique d'où émane la requête.

5. Module selon la revendication 4, dans lequel le droit d'accès est conditionné par la source logique.

6. Dispositif de télécommunication (1) équipé d'un routeur (18) de communication en champ proche et d'un module de sécurité conforme à l'une quelconque des revendications 3 à 5.

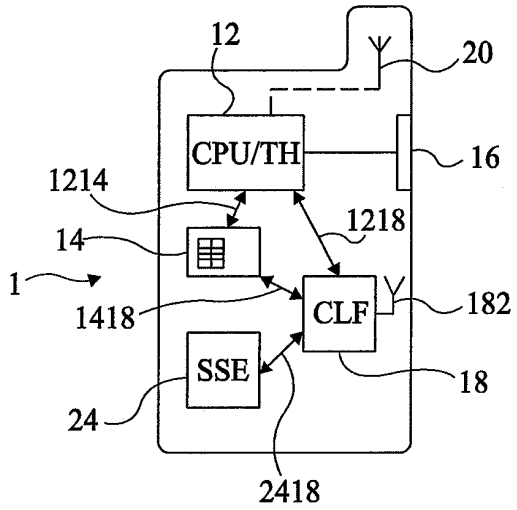

12
20
CPU/TH
16
1214
1218
14
1
1418
CLF
182
SSE
18
24
2418

Fig 1

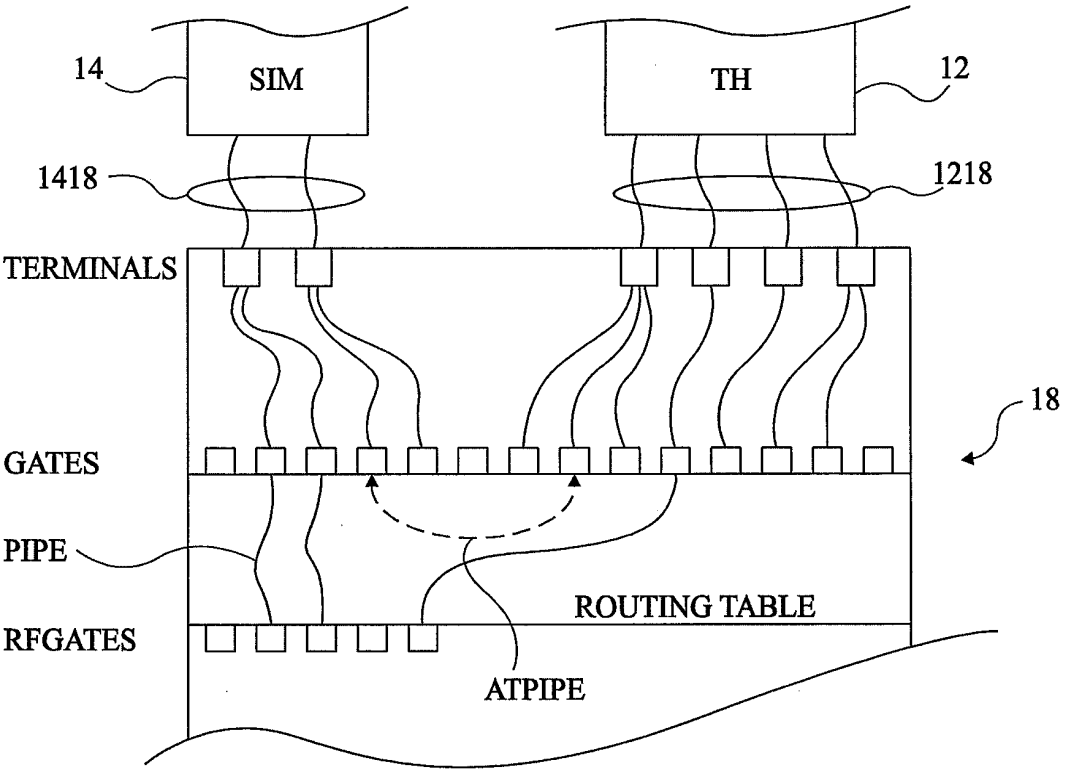

14
SIM
TH
12
1418
1218
TERMINALS
18
GATES
PIPE
ROUTING TABLE
RFGATES
ATPIPE

Fig 2

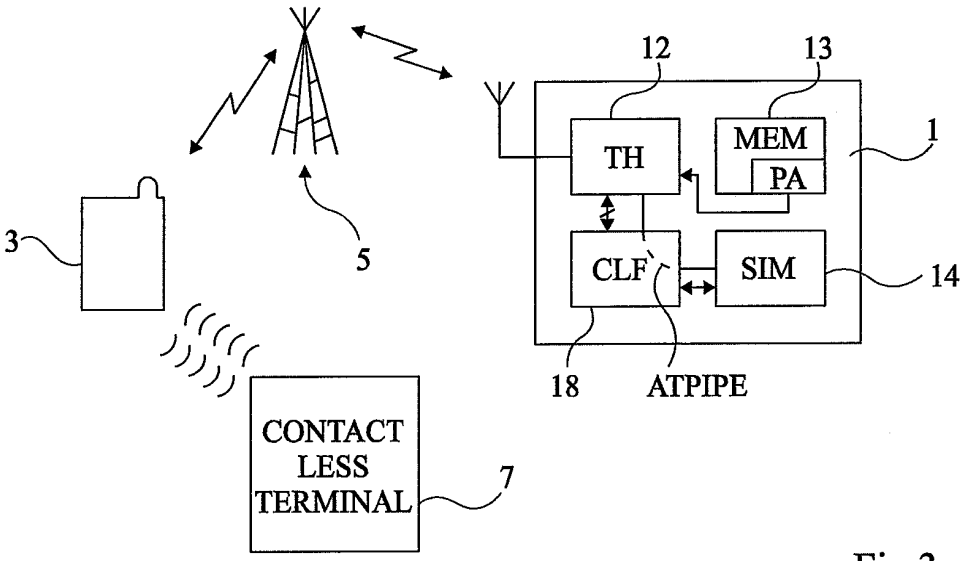

12
13
TH
MEM
PA
1
3
5
CLF
SIM
14
18
ATPIPE
CONTACT
LESS
TERMINAL
7

Fig 3

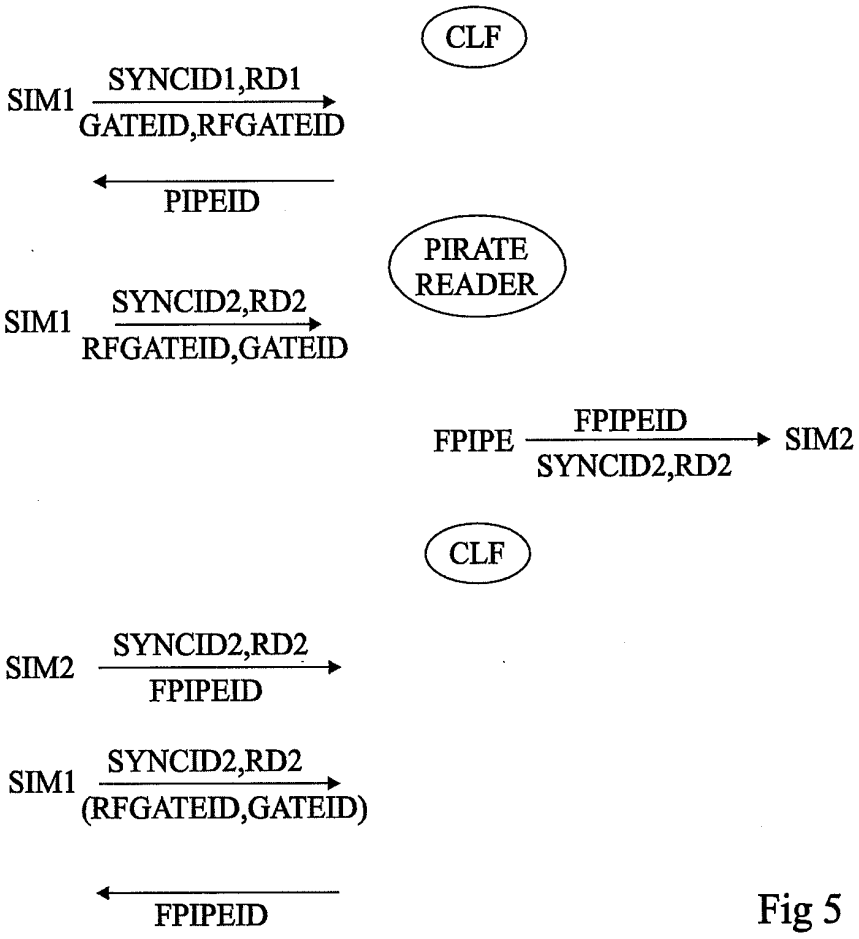

CLF
SIM1
SYNCID1,RD1
GATEID,RFGATEID
PIPEID
PIRATE
READER
SIM1
SYNCID2,RD2
RFGATEID,GATEID
FPIPE
FPIPEID
SYNCID2,RD2
SIM2
CLF
SIM2
SYNCID2,RD2
FPIPEID
SIM1
SYNCID2,RD2
(RFGATEID,GATEID)
FPIPEID

Fig 5

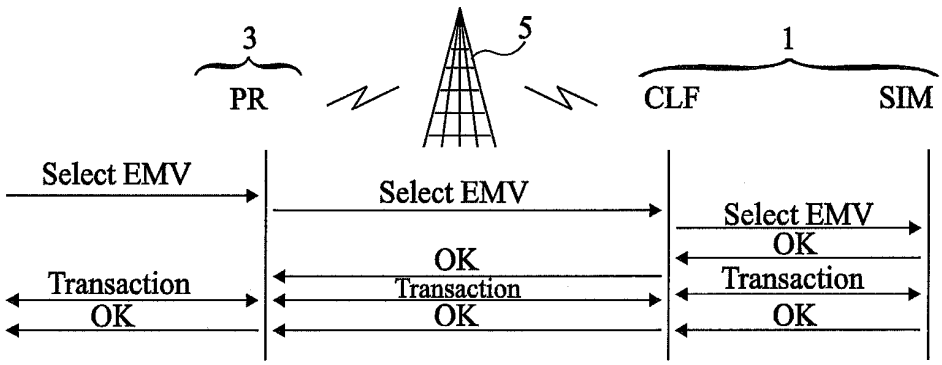


Fig 4

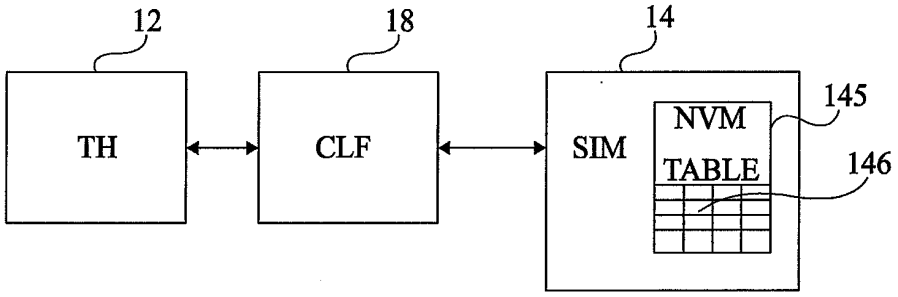


Fig 6

APPLI	Log Source ID	Right
1	00	N
1	02	Y
2	00	N
2	01	Y

146

Fig 7

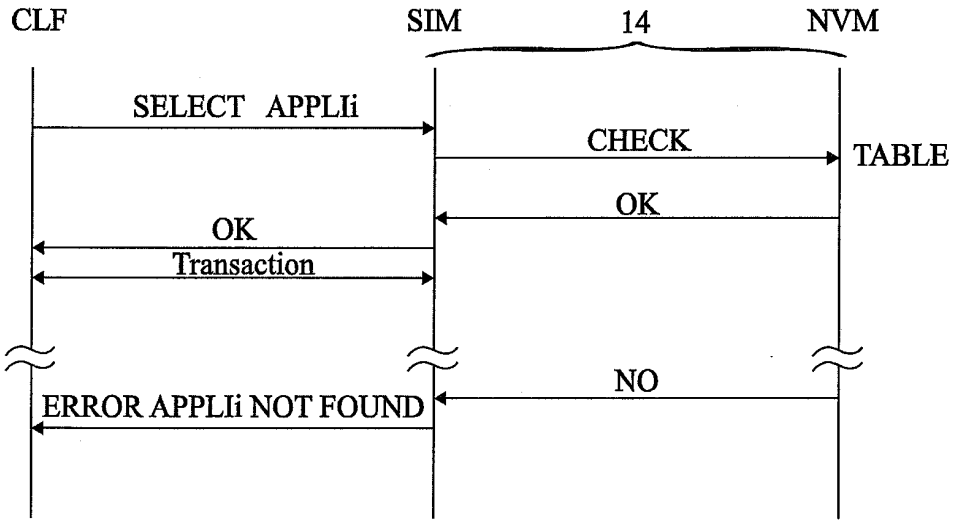

CLF
SIM
14
NVM
SELECT APPLIi
CHECK
TABLE
OK
OK
Transaction
NO
ERROR APPLIi NOT FOUND

Fig 8

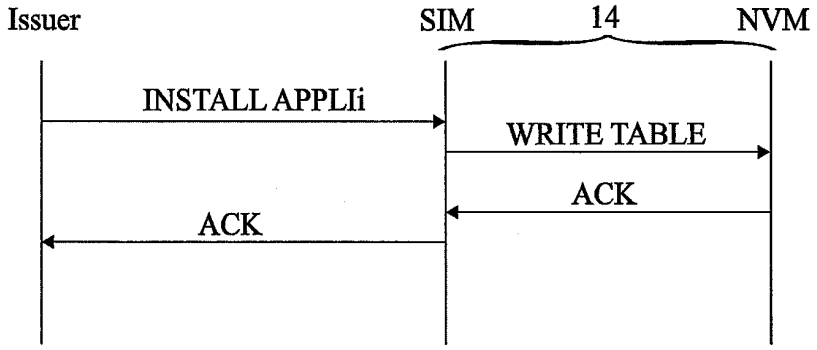

Issuer
SIM
14
NVM
INSTALL APPLIi
WRITE TABLE
ACK
ACK

Fig 9

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 757287
FR 1101134

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 A	WO 2007/068993 A1 (NOKIA CORP [FI]; NYSTROEM SEBASTIAN [FI]; PESONEN LAURI [FI]; SAARISAL) 21 juin 2007 (2007-06-21) * figures 9,10,11 * * page 1, ligne 5 - ligne 7 * * page 1, ligne 18 - ligne 21 * * page 2, ligne 6 - ligne 13 * * page 2, ligne 23 - ligne 32 * * page 3, ligne 10 - page 4, ligne 12 * * page 4, ligne 20 - ligne 28 * * page 4, ligne 33 - ligne 36 * * page 5, ligne 3 - ligne 19 * * page 7, ligne 11 - ligne 19 * * page 7, ligne 33 - ligne 35 * * page 8, ligne 3 - ligne 9 * * page 8, ligne 29 * * page 13, ligne 35 - page 14, ligne 4 * * page 16, ligne 29 - page 17, ligne 32 * * page 25, ligne 5 - page 27, ligne 2 * -----	1-3,6 4,5	G06K17/00 G06Q20/32 H04W12/12
A	MELANIE R RIEBACK ET AL: "Keep on Blockinâ in the Free World: Personal Access Control for Low-Cost RFID Tags", 20 avril 2005 (2005-04-20), SECURITY PROTOCOLS; [LECTURE NOTES IN COMPUTER SCIENCE], SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, PAGE(S) 51 - 59, XP019085239, ISBN: 978-3-540-77155-5 * abrégé * * page 51, ligne 19 - ligne 20 * * page 52, ligne 12 * * page 53, ligne 6 - ligne 30 * * page 53, ligne 32 - page 54, ligne 13 * * tableau 2 * * 3.2 Access Control Lists; page 54 - page 55 * -----	1-6	DOMAINES TECHNIQUES RECHERCHÉS (IPC) H04L G06F

Date d'achèvement de la recherche	Examinateur
11 avril 2012	Oliveira, Joel

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 1101134 FA 757287

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 11-04-2012
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
WO 2007068993 A1	21-06-2007	CN 101297330 A	29-10-2008
		EP 1960974 A1	27-08-2008
		JP 2009519652 A	14-05-2009
		US 2009075592 A1	19-03-2009
		WO 2007068993 A1	21-06-2007

EPO FORM P0465