(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **3 040 226**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **15 57765**

(51) Int Cl[8] : ***G 06 K 19/067*** *(2017.01), H 04 B 5/02*

(12) **BREVET D'INVENTION** **B1**

(54) DISPOSITIF NFC MUNI DE MULTIPLES ELEMENTS SECURISE.

(22) **Date de dépôt :** 17.08.15.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 24.02.17 Bulletin 17/08.

(45) **Date de la mise à disposition du public du brevet d'invention :** 08.06.18 Bulletin 18/23.

(56) **Liste des documents cités dans le rapport de recherche :**

Se reporter à la fin du présent fascicule

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

◯ **Demande(s) d'extension :**

(71) **Demandeur(s) :** *PROTON WORLD INTERNATIONAL N.V.* — BE et *STMICROELECTRONICS (ROUSSET) SAS Société par actions simplifiée* — FR.

(72) **Inventeur(s) :** VAN NIEUWENHUYZE OLIVIER, GRIMAUD JEAN-MARC et MOHAMMED BRAHIM ARACH.

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

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

FR 3 040 226 - B1

DISPOSITIF NFC MUNI DE MULTIPLES ELEMENTS SECURISES

Domaine

La présente description concerne le domaine des communications NFC, et en particulier un dispositif NFC muni de plusieurs éléments sécurisés et un procédé pour router des messages dans un tel dispositif.

Exposé de l'art antérieur

Les téléphones mobiles et d'autres types de dispositifs mobiles sont de plus en plus souvent équipés d'interfaces NFC (de l'anglais Near Field Communication - communication en champ proche), qui leur permettent de réaliser des fonctions de transpondeur électromagnétique en plus de leurs autres fonctions. En particulier, de tels dispositifs sont capables d'émuler les fonctions d'un transpondeur électromagnétique, qui pourrait être du type carte sans contact, ou du type lecteur sans contact. De telles fonctionnalités améliorent par exemple le dispositif mobile en lui permettant d'être utilisé pour diverses applications, par exemple comme portefeuille électronique permettant de réaliser des paiements pour accéder à des services comme des réseaux de transport.

Pour émuler le fonctionnement d'une carte sans contact, le dispositif mobile est en général équipé d'un circuit intégré frontal (CLF), appelé aussi routeur NFC. Ce routeur est

équipé d'un dispositif frontal émetteur-récepteur radiofréquence (RF) couplé à une antenne à faible portée pour s'adapter aux capacités de communication d'un transpondeur électromagnétique. Dans certaines applications, un ou plusieurs éléments sécurisés (SE) ou éléments sécurisés intégrés (eSE), qui sont soit intégrés dans le dispositif mobile soit contenus dans un microcircuit du module USIM (module d'identification d'abonné universel) ou µSD (micro-sécurisé numérique), peuvent être utilisés pour assurer une authentification et d'autres fonctions.

Le routeur NFC comprend une table de routage NFC, qui indique vers quel élément matériel les messages NFC reçus par le routeur NFC doivent être routés. Par exemple, certains messages NFC, comme ceux concernant certains types de paiements électroniques, doivent être routés vers un élément sécurisé du dispositif mobile. Par exemple, une application VISA peut s'exécuter en communication avec un élément sécurisé d'un module USIM (le nom "VISA" peut correspondre à des marques déposées).

Dans certains cas, le dispositif mobile comprend plus qu'un seul élément sécurisé, et il peut y avoir une ou plusieurs applications mémorisées par chaque élément sécurisé qui sont capables de gérer une transaction donnée. Dans un tel cas, il est souhaitable que le dispositif mobile soit capable de sélectionner l'application à utiliser parmi les applications disponibles sur tous les éléments sécurisés.

Toutefois, il y a une difficulté en ce que le routeur NFC n'a pas connaissance de la liste des applications mémorisées par chaque élément sécurisé. En outre lorsqu'un message RF est reçu et a besoin d'être routé vers un élément sécurisé, il n'est pas permis d'interroger, et il n'y a pas non plus le temps pour cela, tous les éléments sécurisés afin d'obtenir les listes des applications disponibles sur chaque élément sécurisé. Il existe donc un besoin dans la technique d'une solution qui réponde à une partie ou à la totalité de ces difficultés.

Résumé

Un objet de modes de réalisation de la présente description est de répondre au moins partiellement à un ou plusieurs besoins de l'art intérieur.

Selon un aspect, on prévoit un procédé comprenant : émuler, par un routeur NFC (communication en champ proche) d'un dispositif NFC, en réponse à une commande provenant d'un dispositif de traitement du dispositif NFC, une transaction d'émulation de carte RF (radiofréquence), l'émulation comprenant l'émission, par le routeur NFC, d'une commande adressée à des premier et deuxième éléments sécurisés du dispositif NFC pour vérifier la présence d'une ou plusieurs applications de transaction NFC dans les premier et deuxième éléments sécurisés ; recevoir, par le routeur NFC, des réponses provenant des premier et deuxième éléments sécurisés indiquant lesdites une ou plusieurs applications de transaction NFC mémorisées par les premier et deuxième éléments sécurisés ; et recevoir, par le routeur NFC, un nouveau message RF provenant d'un terminal NFC concernant une transaction NFC et router le nouveau message RF vers le premier ou le deuxième élément sécurisé en fonction des réponses.

Selon un mode de réalisation, le procédé comprend en outre : générer une liste globale d'applications de transaction NFC disponibles en fonction des réponses ; et fournir la liste globale au terminal NFC en réponse au nouveau message RF.

Selon un mode de réalisation, le procédé comprend en outre, après la génération de la liste globale d'applications de transaction NFC disponibles, la mémorisation de la liste dans une mémoire du routeur NFC.

Selon un mode de réalisation, la liste globale d'applications de transaction NFC disponibles est générée par le dispositif de traitement du dispositif NFC.

Selon un mode de réalisation, lesdites une ou plusieurs applications de transaction NFC sont des applications

de paiement, et la commande comprend une commande de sélection PPSE (environnement de système de paiement de proximité).

Selon un mode de réalisation, chacune desdites ou une plusieurs applications de transaction NFC est associée à une valeur de code système, et la commande comprend un message d'interrogation comprenant une valeur de code système.

Selon un mode de réalisation, le procédé comprend en outre la vérification de la présence d'une ou plusieurs applications de transfert NFC sur les premier et deuxième éléments sécurisés en accédant, par le routeur NFC ou par le dispositif de traitement, à un ou plusieurs bits d'une valeur SAK (accusé de réception de sélection, type A) de chaque élément sécurisé, mémorisée dans un registre du routeur NFC.

Selon un mode de réalisation, le procédé comprend en outre la génération d'une table de routage sur la base desdites réponses, et la mémorisation de la table de routage dans une mémoire du routeur NFC.

Selon un mode de réalisation, le procédé comprend en outre, avant de router le nouveau message RF vers le premier ou le deuxième élément sécurisé, une sélection du premier ou du deuxième élément sécurisé vers lequel le nouveau message RF doit être routé sur la base de la table de routage.

Selon un mode de réalisation, le procédé comprend en outre, avant de router le nouveau message RF vers le premier ou le deuxième élément sécurisé, le fait de répondre au nouveau message RF en communiquant des identificateurs d'au moins deux des applications de transaction au terminal NFC, et recevoir à partir du terminal NFC une sélection de l'une des applications de transaction NFC.

Selon un mode de réalisation, chacun des premier et deuxième éléments sécurisés mémorise une application de transaction de paiement NFC.

Selon un autre aspect, on prévoit un support de stockage numérique mémorisant des instructions qui, lorsqu'elles

sont exécutées par un dispositif de traitement, provoquent la mise en œuvre du procédé susmentionné.

Selon un autre aspect, on prévoit un dispositif NFC (communication en champ proche) comprenant un routeur NFC adapté à : émuler, en réponse à une commande provenant d'un dispositif de traitement du dispositif NFC, une transaction d'émulation de carte RF (radiofréquence), l'émulation de la transaction comprenant l'émission, par le routeur NFC, d'une commande adressée à des premier et deuxième éléments sécurisés du dispositif NFC pour vérifier la présence d'une ou plusieurs applications de transaction NFC dans les premier et deuxième éléments sécurisés ; recevoir des réponses des premier et deuxième éléments sécurisés indiquant lesdites une ou plusieurs applications de transaction NFC mémorisées par les premier et deuxième éléments sécurisés, une liste globale d'applications de transaction NFC disponibles étant générée en fonction des réponses ; et recevoir un nouveau message RF provenant d'un terminal NFC concernant une transaction NFC et router le nouveau message RF vers le premier ou le deuxième élément sécurisé sur la base de la liste globale d'applications de transaction NFC disponibles.

Selon un mode de réalisation, le dispositif de traitement ou le routeur NFC est adapté à générer une liste globale d'applications de transaction NFC disponibles sur la base desdites réponses, et à fournir la liste globale au terminal NFC en réponse au nouveau message RF.

Brève description des dessins

Les caractéristiques et avantages susmentionnés, et d'autres, apparaitront clairement à la lecture de la description détaillée suivante de modes de réalisation donnés à titre d'illustration et non de limitation, en faisant référence aux dessins joints dans lesquels :

la figure 1 illustre schématiquement un dispositif NFC capable de communications NFC selon un exemple de réalisation de la présente description ;

la figure 2 illustre schématiquement le dispositif NFC de la figure 1 plus en détail selon un exemple de réalisation de la présente description ;

la figure 3 illustre schématiquement des composants du dispositif NFC de la figure 2 encore plus en détail selon un exemple de réalisation de la présente description ;

la figure 4 est un organigramme illustrant un exemple d'opérations dans un procédé de routage de messages RF selon un exemple de réalisation de la présente description ;

la figure 5 illustre un exemple d'un paquet de données d'un message NFC de type F selon un exemple de réalisation ; et

la figure 6 illustre une table de routage NFC selon un exemple de réalisation.

Description détaillée

La figure 1 illustre schématiquement un dispositif NFC 102, qui est un dispositif capable de communications NFC. Par exemple, le dispositif 102 est un dispositif mobile, comme un téléphone mobile, un smartphone, une tablette informatique, un lecteur de média numérique ou similaire, équipé de circuits NFC (non illustrés en figure 1).

Sur le côté gauche de la figure 1, le dispositif NFC 102 est représenté en communication avec un lecteur 104, comprenant un transpondeur NFC 106. Par exemple, le lecteur 104 est disposé au niveau d'une barrière d'entrée d'une zone à accès limité, comme un réseau de transport ou similaire. En variante, le lecteur 104 peut être disposé au niveau d'un point de vente dans un magasin ou un restaurant. Lorsqu'elle est utilisée avec un tel lecteur, la circuiterie NFC du dispositif NFC 102 fonctionne par exemple dans un mode d'émulation d'étiquette.

Sur le côté droit de la figure 1, le dispositif NFC 102 est représenté en communication avec un autre dispositif NFC 108 par l'intermédiaire d'une interface NFC. Par exemple, comme le dispositif NFC 102, le dispositif NFC 108 est un dispositif capable de communications NFC, qui pourrait être un dispositif mobile comme un téléphone mobile, un smartphone, une tablette

informatique, un lecteur de média numérique ou similaire, équipé d'une circuiterie NFC. Lors d'une communication avec un autre dispositif NFC, la circuiterie NFC du dispositif NFC 102 fonctionne par exemple dans un mode de poste à poste, et des communications sont lancées par l'un ou l'autre des dispositifs NFC.

La figure 2 illustre schématiquement le dispositif NFC 102 plus en détail selon un exemple de réalisation.

Comme cela est illustré, le dispositif 102 comprend par exemple un routeur NFC (NFC ROUTER) 202, aussi connu dans la technique sous le nom de frontal sans contact (CLF). Le routeur NFC 202 est couplé à une antenne NFC 204, et ensemble le routeur 202 et l'antenne 204 assurent une circuiterie NFC pour émuler le comportement d'un transpondeur NFC.

Le routeur NFC 202 est aussi par exemple couplé à un dispositif de traitement hôte (P) 206 du dispositif NFC 102. Le dispositif 206 comprend par exemple un ou plusieurs processeurs sous le contrôle d'instructions mémorisées dans une mémoire d'instructions (INSTR MEM) 208. La mémoire d'instructions 208 est par exemple une mémoire flash, et mémorise une ou plusieurs applications (non illustré en figure 2), qui ont été chargées dans le dispositif. Le routeur NFC 202 est aussi par exemple couplé à d'autres dispositifs, parmi lesquels un élément sécurisé (SE) 210 et un circuit USIM 212 (module d'identification d'abonné universel) sont illustrés. L'élément sécurisé 210 est par exemple un SE intégré (eSE) couplé au routeur NFC par intermédiaire d'une liaison SWP (protocole à un seul fil) et le circuit USIM 212 est par exemple une carte UICC (carte de circuit intégré universelle) couplée au routeur NFC par l'intermédiaire d'une liaison SWP, et est couplé additionnellement au dispositif de traitement hôte 206. Bien que cela ne soit par illustré en figure 2, il peut y avoir d'autres éléments sécurisés comme un ou plusieurs µSD.

Le dispositif de traitement hôte 206 est aussi par exemple couplé à une ou plusieurs antennes 214, qui permettent

des télécommunications dans un réseau cellulaire, et/ou des communications sans fil conformément à d'autres normes comme les normes Wifi, Bluetooth, etc.

Le routeur NFC 202 comprend par exemple une ou plusieurs mémoires mémorisant une table de routage NFC 218 et une liste PPSE 220 (environnement de système de paiement de proximité) d'applications de transaction de paiement NFC disponibles mémorisées par les éléments sécurisés 210, 212, comme cela sera décrit plus en détail ci-après. La table de routage NFC 218 définit des règles pour le traitement de messages NFC reçus par le routeur NFC 202. En particulier, les messages peuvent être considérés comme étant adressés soit au dispositif de traitement 206 soit à l'un des éléments sécurisés 210, 212. Lesdites une ou plusieurs mémoires du routeur NFC 202 mémorisent aussi par exemple un registre 221 dans lequel une valeur SAK (accusé de réception de sélection, type A) est par exemple mémorisée en association avec chaque élément sécurisé, comme on va le décrire plus en détail ci-après.

En fonctionnement, la table de routage 218 pourrait être configurée pour router toutes les communications RF associées à des paiements vers un élément sécurisé spécifique, comme l'élément 210. Dans un tel cas, lorsque le dispositif NFC 102 vient dans la portée d'un terminal NFC, comme le terminal 104 de la figure 1, le terminal émet un message d'interrogation RF vers le dispositif NFC. Le routeur NFC 202 détecte par exemple, sur la base d'un identificateur dans le message d'interrogation, que la communication concerne un paiement, et sur la base de la table de routage NFC 218, route automatiquement la communication vers un élément sécurisé approprié, comme l'élément 210. Le terminal NFC transmet ensuite une commande de sélection Select PPSE à l'élément sécurisé. Une application PPSE de l'élément sécurisé répond en fournissant une liste d'applications de paiement disponibles sur l'élément sécurisé, avec leurs identificateurs d'application (AID). Les applications de paiement sont par exemple présentées au terminal

NFC dans un ordre de préférence défini par l'utilisateur. Le terminal NFC sélectionne ensuite une application de paiement appropriée sur la base des capacités du terminal NFC. Dans le cas où il y a plus qu'une seule application de paiement dans l'élément sécurisé 210 qui est compatible avec le terminal NFC, le terminal NFC sélectionne par exemple l'application ayant la priorité la plus haute. En particulier, un utilisateur du dispositif NFC a par exemple indiqué une priorité parmi les applications de paiement avant que la transaction soit exécutée. La priorité est par exemple représentée par l'ordre des transactions dans la liste renvoyée par l'application PPSE, l'application la plus haute dans la liste ayant la priorité la plus haute, et l'application la plus basse dans la liste ayant la priorité la plus basse.

La transaction de paiement va ensuite être exécutée en utilisant l'application hébergée par l'élément sécurisé qui a la priorité la plus haute et qui est supportée par le terminal NFC. Dans un exemple particulier, l'application ayant la priorité la plus haute est une application de paiement "nationale", liée par exemple au compte bancaire du dispositif de l'utilisateur, et une application de priorité inférieure est une application de paiement "internationale", comme une application VISA. Un terminal NFC se situant dans le pays d'origine de l'utilisateur va ainsi par exemple supporter à la fois les applications nationales et les applications internationales, et l'application nationale va être sélectionnée au vu de sa priorité supérieure. Un terminal NFC se trouvant dans un autre pays ne prend pas en charge l'application nationale, et ainsi l'application internationale va être sélectionnée pour exécuter la transaction.

La procédure susmentionnée fonctionne bien lorsqu'il y a un seul élément sécurisé capable de gérer un type de transaction donné. Toutefois, dans certain cas, il peut y avoir plus qu'un seul élément sécurisé sur le dispositif NFC qui est capable de réaliser cela. Par exemple, les éléments sécurisés 210 et 212 peuvent tous les deux mémoriser des applications

capables de gérer des paiements ou d'autres types de transactions, comme on va le décrire maintenant en faisant référence à la figure 3.

La figure 3 illustre schématiquement des composants du dispositif NFC de la figure 2 plus en détail selon un exemple de réalisation. En particulier, la figure 3 illustre le routeur NFC (NFC ROUTER) 202, l'hôte de dispositif (DEVICE HOST) 206, et les éléments sécurisés (SE1) 210 et (SE2) 212. Les deux éléments sécurisés 210, 212 mémorisent par exemple une application PPSE (environnement de système de paiement de proximité). En outre, l'élément sécurisé 210 mémorise par exemple des applications de transaction NFC APP1 et APP2, et l'élément sécurisé 212 mémorise par exemple des applications de transaction NFC APP2 et APP3. Le terme "application de transaction NFC" est utilisé ici pour désigner une application qui est exécutée sur un élément sécurisé et qui permet à une transaction d'avoir lieu par l'intermédiaire de l'interface NFC, comme une transaction de paiement sécurisée, ou une autre forme de transaction financière ou privée.

Les applications APP1 et APP3 sont par exemple des applications de paiement, APP1 étant par exemple une application VISA, et APP3 étant par exemple une application MasterCard (le nom "MasterCard" peut correspondre à un nom de marque déposé).

Les applications APP2 dans les deux éléments sécurisés sont par exemple identiques. Toutefois, elles sont par exemple configurées pour des comptes et/ou des circonstances de paiement de nature différente. Par exemple, les deux applications APP2 sont des applications de paiement de transfert comme les applications MIFARE Classic 1K (le nom MIFARE est susceptible de correspondre à un nom de marque déposé). Toutefois, ces applications peuvent être configurées pour une utilisation sur des réseaux de transport différents, et/ou dans des pays différents.

Sur la base d'un message d'interrogation RF provenant d'un terminal NFC et concernant une transaction de paiement ou

de transfert, le routeur NFC 202 n'est pas capable de déterminer lequel des éléments sécurisés doit être utilisé pour mettre en œuvre la transaction.

La figure 4 est un organigramme d'un procédé de routage d'un message RF selon un exemple de réalisation. Le procédé comprend par exemple des opérations 401 à 404 pour générer une liste globale d'applications NFC disponibles, et une opération 405 dans laquelle la liste d'applications disponibles est fournie à un terminal NFC en réponse à un nouveau message RF. Les données destinées à former la liste globale d'applications de transaction NFC disponibles sont par exemple recueillies par le retour NFC 202 en réponse à une commande du dispositif hôte 206, et intègrent des données récupérées à partir de chaque élément sécurisé et optionnellement à partir d'autres sources.

Dans une opération 401, une commande est émise à partir du dispositif hôte 206 à destination du routeur NFC 202, pour générer une liste globale d'applications de transaction NFC disponibles. Cette commande est par exemple générée périodiquement, par exemple toutes les heures, de sorte que la liste d'applications disponibles est toujours relativement à jour. Dans certains modes de réalisation, une commande est générée en réponse à la détection par le dispositif hôte d'un nouvel identificateur d'application AID mémorisé par le dispositif hôte pour refléter un changement dans les applications, comme l'ajout d'une nouvelle application.

Dans une opération 402, le routeur NFC 202 obtient par exemple des détails d'applications de paiement sur un premier élément sécurisé du dispositif NFC en réalisant une émulation d'une session d'émulation de carte RF. Par exemple, le premier élément est l'élément 210. L'émulation est par exemple une émulation de carte en mode interface contrôleur hôte (HCI), et implique de demander une liste d'applications au premier élément sécurisé. Par exemple, l'émulation est basée sur une communication selon le type A ou le type B définis par la norme NFC

ISO/IEC 14443. Cette étape implique par exemple l'émulation d'une transaction d'émulation de carte RF en envoyant une commande HCI, comme cela est défini dans la spécification ETSI TS 102 622. Par exemple, une version V12.1.0 de cette spécification ETSI (Institut Européen des Normes de Télécommunications) est disponible sur le site web http://www.etsi.org, dont le contenu est considéré comme inclus ici dans les limites autorisées par la loi. En particulier, l'émulation d'une transaction d'émulation de carte RF comprend par exemple l'activation, par le routeur NFC 202, d'une liaison de communication entre le routeur NFC 202 et le premier élément sécurisé, si cette liaison est désactivée. La liaison de communication entre le routeur NFC 202 et chaque élément sécurisé est par exemple une liaison SWP (protocole à un seul fil).

Le routeur NFC 202 demande ensuite par exemple, au premier élément sécurisé du dispositif NFC, une liste d'applications de paiement qui sont mémorisées par celui-ci et qui sont disponibles pour gérer des transactions NFC. Par exemple, cette demande prend la forme d'une commande "SELECT PPSE" transmise par le routeur NFC 202 au premier élément sécurisé du dispositif NFC. La réalisation d'une commande SELECT PPSE implique par exemple d'abord l'envoi d'un message d'évènement EVT_CARD_ACTIVATION sur la base d'une émulation de carte du type RF A ou B, en fonction de la configuration de l'élément sécurisé. Cet évènement est défini par la spécification ETSI TS 102 622. Le message est par exemple basé sur une structure de message HCP (Protocole de Contrôleur Hôte) ayant le format suivant :

Entête : un octet (bits b1 à b8)

- type : b8, b7
- instruction : b6 à b1

Données : taille non limitée (mais par exemple découpée en paquets pour transmission sur le SWP conformément à la spécification ETSI TS 102 613).

Par exemple les huit bits du EVT_SEND_DATA sont 0x50.

Comme pour une vraie transaction RF, la commande encapsule par exemple une requête d'application Select PPSE ISO7816 appelée EVT_SEND_DATA, tel que défini par la spécification ETSI TS 102 622. On trouvera ci-après un exemple spécifique des valeurs hexadécimales formant une commande ISO-Select à inclure dans une commande EVT_SEND_DATA pour sélectionner le PPSE (valeur de CRC retirée) :
"00 a4 04 00 0e 32 50 41 59 2e 53 59 53 2e 44 44 46 30 31 00"

Une application mémorisée par le premier élément sécurisé, qui est par exemple une application PPSE, répond par exemple à la requête Select PPSE en fournissant une liste de toutes les applications de transaction de paiement NFC disponibles mémorisées par l'élément sécurisé. La réponse est par exemple une réponse APDU (bloc de données de protocole d'application), qui est par exemple aussi encapsulée dans une commande HCI EVT_SEND_DATA. A titre d'exemple spécifique dans lequel une application de paiement Interac est présente sur l'élément sécurisé (le nom "Interac" peut correspondre à une ou plusieurs noms de marques déposés), la réponse à la commande Select PPSE susmentionnée est par exemple le message suivant, présenté sous forme de valeurs hexadécimales, sur la base d'un exemple dans lequel il y a une seule application de paiement :
"6F 2C 84 0E 32 50 41 59 2E 53 59 53 2E 44 44 46 30 31 A5 1A BF 0C 17 61 15 4F 07 A0 00 00 02 77 10 10 87 01 01 50 07 49 4E 54 45 52 41 43". Cette réponse peut être analysée de la façon suivante :

PICC Succès
Données (46 octets)
Étiquette 6F : Modèle FCI
Longueur : 2C
Étiquette 84 : Nom fichier dédié (DF)
Longueur : 0E
Valeur : 32 50 41 59 2E 53 59 53 2E 44 44 46 30 31
Étiquette A5 : Modèle propriétaire FCI *(première application)*

Longueur : 1A
Étiquette BF0C : Données discrétionnaires FCI
Longueur : 17
Étiquette 61 : Modèle d'application
Longueur : 15
Étiquette 4F : Identificateur d'application
Longueur : 07
Valeur : A0 00 00 02 77 10 10
Étiquette 87 : Indicateur de priorité d'application
Longueur : 01
Valeur : 01
Étiquette 50 : Etiquette d'application
Longueur : 07
Valeur : 49 4E 54 45 52 41 43
Valeur ASCII: INTERAC
Étiquette A5 : Modèle propriétaire FCI *(deuxième application)*
.....*etc.*
SW1 SW2 : 90 00

où PICC signifie carte à circuit intégré de proximité. Comme cela est illustré dans cet exemple, la portion Étiquette A5 est par exemple répétée pour chaque application qui se trouve sur l'élément sécurisé. L'homme de l'art comprendra qu'un ou plusieurs des champs de cette réponse peuvent être optionnels et qu'un ou plusieurs champs additionnels peuvent être présents, en fonction de l'application. La réponse indique par exemple au moins l'identificateur d'application AID de chaque application de transaction de paiement qui est présente. Le format de la commande et la façon dont elle doit être analysée sont par exemple décrits plus en détail dans la spécification EMVCo, et en particulier dans le document EMV Contactless, Book B (version 2.5), table 3-2, dont le contenu entier est considéré comme inclus ici dans les limites autorisées par la loi.

L'utilisation de la commande Select PPSE telle que décrite précédemment permet à l'application PPSE mémorisée sur les éléments sécurisés de fournir des informations concernant des applications de paiement. Dans certains modes de réalisation, le routeur NFC 202 ou le dispositif hôte 206 est aussi adapté à obtenir des informations concernant d'autres types d'applications mémorisées par les éléments sécurisés.

Par exemple, pour des applications de transfert telles que MIFARE Classic, le routeur NFC ou le dispositif hôte lit par exemple une partie d'une valeur SAK (accusé de réception de sélection, type A) que l'élément sécurisé mémorise dans un registre du routeur NFC 202. En particulier, un bit de la valeur SAK indique par exemple le moment où une application MIFARE Classic, ou une application similaire selon la norme ISO/IEC 14443 partie 3, est présente sur l'élément sécurisé.

Pour des applications comme les applications FeliCa associées à un code système, une émulation de carte de type F est par exemple utilisée avec certains codes système pour vérifier si certaines applications sont présentes sur un élément sécurisé. En particulier, le routeur NFC émet par exemple une requête d'interrogation vers l'élément sécurisé contenant un code système, et reçoit une réponse indiquant si une application associée à ce code de système se trouve ou pas sur l'élément sécurisé. Cette opération est par exemple répétée jusqu'à obtenir un ou plusieurs résultats positifs permettant d'identifier une ou plusieurs applications FeliCa, ou des applications similaires comprenant un SAK.

La figure 5 illustre un exemple du format d'un message d'interrogation de type F selon la norme NFC ISO/IEC 18092. Comme cela est illustré, le paquet de données comprend par exemple un préambule (PRE) 502 qui a par exemple une longueur de 38 bits ou plus, un champ de synchronisation (SYNC) 504, qui a par exemple une longueur de 6 bits ou plus, un champ de longueur (L) 506, qui a par exemple une longueur de 8 bits et qui indique la longueur totale de la trame, une charge utile (PAYLOAD) 508,

et un champ de code de redondance cyclique (CRC) 509. La charge utile 508 comprend par exemple des sous-champs comprenant un code d'instruction (INS) 510, et un ou plusieurs champs de données. La figure 5 illustre le cas d'un message d'interrogation dans lequel les champs de données comprennent deux champs de code système (SC1, SC2) 512 et 514 qui sont destinés à sélectionner une application spécifique, un champ de code de requête (RC) 516 utilisé pour demander des informations additionnelles, et un numéro de créneau temporel TSN 518 utilisé dans un but d'anticollision dans le cas où plusieurs cartes sont présentes dans le champ.

Dans le cas d'un message d'interrogation, les valeurs des champs PRE et SYNC ne sont pas, par exemple, prise en compte puisqu'elles sont utilisées pour détecter le début de trame et la vitesse de transmission. Les autres champs ont par exemple les valeurs hexadécimales suivantes : 06 00 FF FF 00 00 09 21, où le code d'instruction INS 510 est par exemple égal à 0x00, et les champs 512 et 514 sont tous deux par défaut à la valeur 0xFF, correspondant à des valeurs génériques, ce qui signifie que toutes les autres valeurs sont acceptées (le préfixe "0x" est utilisé ici pour indiquer que les caractères correspondent à des valeurs hexadécimales). Un autre exemple du champ de code système SC1, SC2 est 0x00 0x02.

En faisant de nouveau référence à la figure 4, dans une opération suivante 403, on détermine s'il y a ou pas d'autres éléments sécurisés à accéder. Dans l'exemple de la figure 3, il y a deux éléments sécurisés 210, 212, et ainsi après que l'élément sécurisé 210 a été accédé, il y aura encore un autre élément sécurisé 212 restant.

S'il y a un autre élément sécurisé n'ayant pas encore été accédé, le procédé revient par exemple à l'opération 402, et cette opération est répétée pour l'autre élément sécurisé.

Une fois que tous les éléments sécurisés ont été accédés, l'opération suivante est l'opération 404, dans laquelle une liste globale 220 d'applications de transaction NFC est par

exemple construite par le routeur NFC 202, sur la base des listes d'applications fournies par chaque élément sécurisé. Par exemple, la liste globale 220 d'applications correspond à une liste globale d'applications PPSE, qui liste les applications de paiement NFC présentes sur les éléments sécurisés. Une telle liste a par exemple le même format que la réponse PPSE provenant de chaque élément sécurisé (voir l'exemple de la réponse APDU donné ci-avant), mais liste les applications mémorisées par chacun des éléments sécurisés du dispositif NFC. Cette liste est ensuite par exemple mémorisée dans une mémoire du routeur NFC.

Plutôt que d'être générée par le routeur NFC 202, dans certains modes de réalisation la liste globale d'applications 220 pourrait être générée par l'hôte de dispositif 206 si par exemple le routeur NFC 202 communique les listes d'applications fournies par les éléments sécurisés au dispositif hôte 206. En outre, plutôt que d'être mémorisée par le routeur NFC, la liste 220 pourrait être mémorisée par une mémoire de l'hôte de dispositif 206.

Le routeur NFC 202 ou l'hôte de dispositif 206 génère aussi par exemple, ou modifie, la table de routage NFC 218, sur la base des applications identifiées mémorisées par chaque élément sécurisé.

La figure 6 est une table illustrant un exemple de la table de routage NFC 218.

Dans l'exemple de la figure 6, la table de routage 218 comporte cinq entrées. La première entrée ENTRY1 correspond par exemple à une application de paiement VISA ayant un identificateur d'application en hexadécimal de "A0000000031010", et située dans l'UICC 212, l'UICC 212 étant ainsi la cible pour des messages adressés à cette application. La deuxième entrée ENTRY2 correspond par exemple à une application FeliCa ayant un code système en hexadécimal de "0002", et située dans l'UICC 212, l'UICC 212 étant ainsi la cible pour des messages adressés à cette application. La troisième entrée ENTRY3 correspond par exemple à une application MasterCard ayant un identificateur

d'application en hexadécimal de "A0000000041010", et située dans l'eSE 210, l'eSE 210 étant ainsi la cible pour des messages adressés à cette application. La quatrième entrée ENTRY4 correspond par exemple à une application MIFARE Classic, qui utilise un routage RF de type A et n'est associée à aucun AID ou code système, et qui est située dans l'eSE 210, l'eSE 210 étant ainsi la cible pour des messages adressés à cette application. La cinquième entrée ENTRY5 correspond par exemple à une application FeliCa ayant un code système en hexadécimal "0003", et qui est située dans l'eSE 210, l'eSE 210 étant ainsi la cible pour des messages adressés à cette application.

Lors de la génération de la table de routage 218 et de la liste globale 220 d'applications de transaction NFC, une vérification est par exemple réalisée pour éviter des conflits entre les applications. Par exemple, s'il y a plus qu'une seule application de paiement identifiée comme ayant le même identificateur d'application AID, une sélection est faite afin qu'une seule de ces applications n'apparaisse dans la liste d'applications 220 et dans la table de routage 218. Par exemple, l'utilisateur du dispositif NFC est invité par l'hôte de dispositif 206 à faire cette sélection. En outre, si plus qu'une seule application de transfert est identifiée mémorisée sur les éléments sécurisés, de nouveau une sélection est par exemple faite parmi les applications, par exemple en invitant l'utilisateur à faire cette sélection.

En référence de nouveau à la figure 4, dans l'opération 405 qui peut avoir lieu à tout instant après que la liste globale d'applications NFC a été construite dans l'opération 404, un nouveau message RF est reçu d'un terminal NFC, et routé sur la base de la liste globale construite d'applications de transaction NFC 220 et/ou sur la base de la table de routage 218.

Par exemple, si la liste 220 n'inclut qu'une seule application de transaction NFC capable de gérer la transaction RF donnée, le routeur NFC 202 route par exemple le message RF

directement vers l'élément sécurisé sur lequel l'application de transaction NFC est mémorisée.

Autrement, si la liste 220 comprend plus qu'une seule application de transaction NFC capable de gérer la transaction RF, alors le routeur NFC 202 répond par exemple au terminal NFC avec un message comprenant les identificateurs NFC des applications de transaction disponibles qui peuvent gérer la transaction NFC. Par exemple, le terminal NFC émet une commande SELECT PPSE vers le routeur NFC, et le routeur NFC répond directement au terminal NFC en transmettant une liste d'applications de paiement NFC disponibles dans les éléments sécurisés. S'il n'y a qu'une seule application de transaction NFC qui est compatible avec le terminal NFC, le terminal NFC sélectionne par exemple cette application de transaction NFC. Autrement, s'il y a plus qu'une seule application de transaction qui est compatible avec le terminal NFC, alors le terminal NFC sélectionne par exemple l'application ayant la priorité la plus haute, qui est par exemple l'application la plus haute sur la liste PPSE. Le routeur NFC 202 envoie ensuite par exemple un nouveau message RF à l'application de transaction sélectionnée, qui est routé par le routeur NFC 202 vers l'élément sécurisé mémorisant l'application de transaction NFC.

Plutôt que la liste globale 220 d'applications de transaction soit mémorisée par le routeur NFC 202, comme cela a été mentionné précédemment, dans certains modes de réalisation cette liste pourrait être mémorisée par une mémoire du dispositif hôte 206. Dans ce cas, la table de routage 218 du routeur NFC 202 est par exemple configurée pour router des requêtes SELECT PPSE reçues de terminaux NFC vers le dispositif hôte 206, de sorte que le dispositif hôte de 206 peut répondre à de telles requêtes en fournissant la liste 220 d'applications de paiement mémorisées par les éléments sécurisés.

Un avantage des modes de réalisation décrits ici est qu'on peut faire une sélection entre plusieurs applications de transaction NFC mémorisées par des éléments sécurisés différents

lorsqu'un nouveau message NFC est reçu. Cela est obtenu en construisant une liste globale d'applications de transaction NFC disponibles d'une manière sûre en émulant, en réponse à une commande provenant du dispositif hôte, une transaction d'émulation de carte RF.

Avec la description ainsi faite d'un mode de réalisation illustratif, diverses altérations, modifications et améliorations apparaîtront facilement à l'homme de l'art.

Par exemple, bien que dans les exemples les applications de transaction mémorisées par les éléments sécurisés soient des applications de paiement, il apparaitra clairement à l'homme de l'art que les applications pourraient être destinées à la réalisation d'autres types de transactions.

En outre, il apparaitra clairement à l'homme de l'art que les divers éléments décrits en relation avec les divers modes de réalisation peuvent être combinés, dans des variantes de réalisation, selon diverses combinaisons.

REVENDICATIONS

1. Procédé comprenant :

émuler, par un routeur NFC (communication en champ proche) (202) d'un dispositif NFC (102), en réponse à une commande provenant d'un dispositif de traitement (206) du dispositif NFC, une transaction d'émulation de carte RF (radiofréquence), l'émulation comprenant l'émission, par le routeur NFC (202), d'une commande adressée à des premier et deuxième éléments sécurisés (210, 212) du dispositif NFC pour vérifier la présence d'une ou plusieurs applications de transaction NFC dans les premier et deuxième éléments sécurisés ;

recevoir, par le routeur NFC (202), des réponses provenant des premier et deuxième éléments sécurisés (210, 212) indiquant lesdites une ou plusieurs applications de transaction NFC mémorisées par les premier et deuxième éléments sécurisés ; et

recevoir, par le routeur NFC (202), un nouveau message RF provenant d'un terminal NFC (106) concernant une transaction NFC et router le nouveau message RF vers le premier ou le deuxième élément sécurisé en fonction des réponses.

2. Procédé selon la revendication 1, comprenant en outre :

générer une liste globale (220) d'applications de transaction NFC disponibles en fonction des réponses ; et

fournir la liste globale (220) au terminal NFC en réponse au nouveau message RF.

3. Procédé selon la revendication 2, comprenant en outre, après la génération de la liste globale (220) d'applications de transaction NFC disponibles, la mémorisation de la liste dans une mémoire du routeur NFC (202).

4. Procédé selon la revendication 2 ou 3, dans lequel la liste globale (220) d'applications de transaction NFC disponibles est générée par le dispositif de traitement (206) du dispositif NFC.

5. Procédé selon l'une quelconque des revendications 1 à 4, dans lequel lesdites une ou plusieurs applications de transaction NFC sont des applications de paiement, et dans lequel la commande comprend une commande de sélection PPSE (environnement de système de paiement de proximité).

6. Procédé selon l'une quelconque des revendications 1 à 5, dans lequel chacune desdites ou une plusieurs applications de transaction NFC est associée à une valeur de code système, et la commande comprend un message d'interrogation comprenant une valeur de code système.

7. Procédé selon l'une quelconque des revendications 1 à 6, comprenant en outre la vérification de la présence d'une ou plusieurs applications de transfert NFC sur les premier et deuxième éléments sécurisés en accédant, par le routeur NFC (202) ou par le dispositif de traitement (206), à un ou plusieurs bits d'une valeur SAK (accusé de réception de sélection, type A) de chaque élément sécurisé mémorisée dans un registre (221) du routeur NFC (202).

8. Procédé selon l'une quelconque des revendications 1 à 7, comprenant en outre la génération d'une table de routage (218) sur la base desdites réponses, et la mémorisation de la table de routage dans une mémoire du routeur NFC (202).

9. Procédé selon la revendication 8, comprenant en outre, avant de router le nouveau message RF vers le premier ou le deuxième élément sécurisé (210, 212), une sélection du premier ou du deuxième élément sécurisé vers lequel le nouveau message RF doit être routé sur la base de la table de routage (218).

10. Procédé selon l'une quelconque des revendications 1 à 9, comprenant en outre, avant de router le nouveau message RF vers le premier ou le deuxième élément sécurisé (210, 212), le fait de répondre au nouveau message RF en communiquant des identificateurs d'au moins deux des applications de transaction au terminal NFC (106), et recevoir à partir du

terminal NFC une sélection de l'une des applications de transaction NFC.

11. Procédé selon l'une quelconque des revendications 1 à 10, dans lequel chacun des premier et deuxième éléments sécurisés (210, 212) mémorise une application de transaction de paiement NFC.

12. Support de stockage numérique mémorisant des instructions qui, lorsqu'elles sont exécutées par un dispositif de traitement, amènent la mise en œuvre du procédé de l'une quelconque des revendications 1 à 11.

13. Dispositif NFC (communication en champ proche) comprenant :

un routeur NFC (202) adapté à :

émuler, en réponse à une commande provenant d'un dispositif de traitement (206) du dispositif NFC, une transaction d'émulation de carte RF (radiofréquence), l'émulation de la transaction comprenant l'émission, par le routeur NFC (202), d'une commande adressée à des premier et deuxième éléments sécurisés (210, 212) du dispositif NFC pour vérifier la présence d'une ou plusieurs applications de transactions NFC dans les premier et deuxième éléments sécurisés ;

recevoir des réponses des premier et deuxième éléments sécurisés (210, 212) indiquant lesdites une ou plusieurs applications de transaction NFC mémorisées par les premier et deuxième éléments sécurisés, une liste globale (220) d'applications de transaction NFC disponibles étant générée en fonction des réponses ; et

recevoir un nouveau message RF provenant d'un terminal NFC (106) concernant une transaction NFC et router le nouveau message RF vers le premier ou le deuxième élément sécurisé sur la base de la liste globale d'applications de transaction NFC disponibles.

14. Dispositif selon la revendication 13, dans lequel le dispositif de traitement (206) ou le routeur NFC (202) est adapté à générer une liste globale (220) d'applications de

transaction NFC disponibles sur la base desdites réponses, et à fournir la liste globale (220) au terminal NFC en réponse au nouveau message RF.

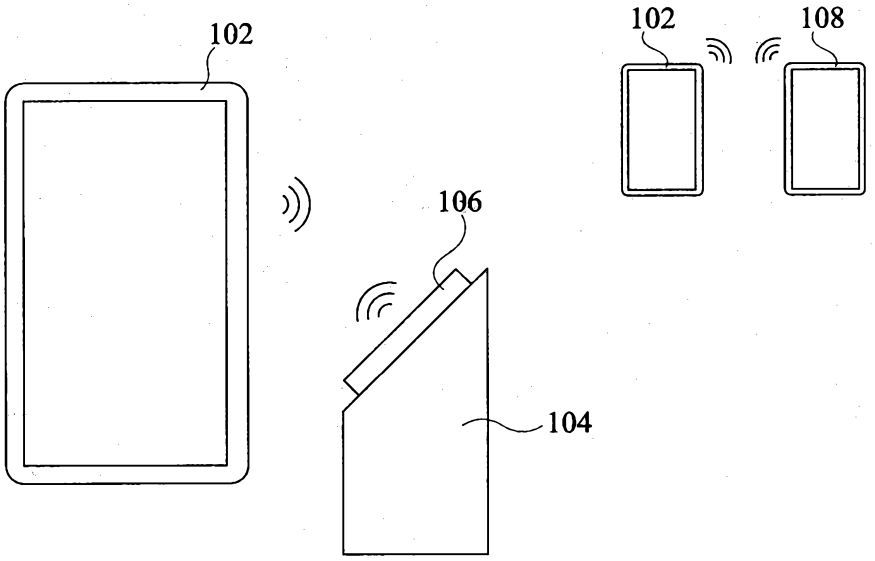
102
102
108
106
104

Fig 1

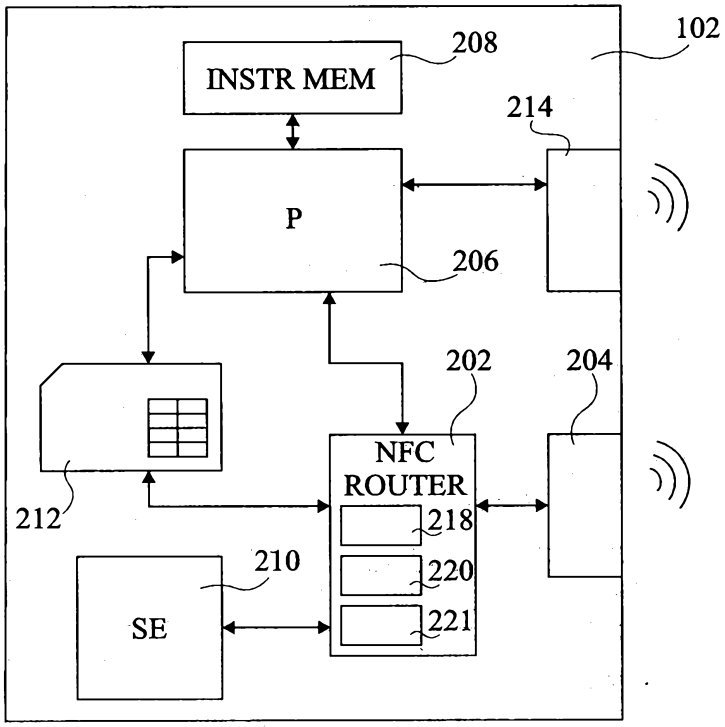
102
INSTR MEM
208
214
P
206
202
204
NFC
ROUTER
212
218
220
221
210
SE

Fig 2

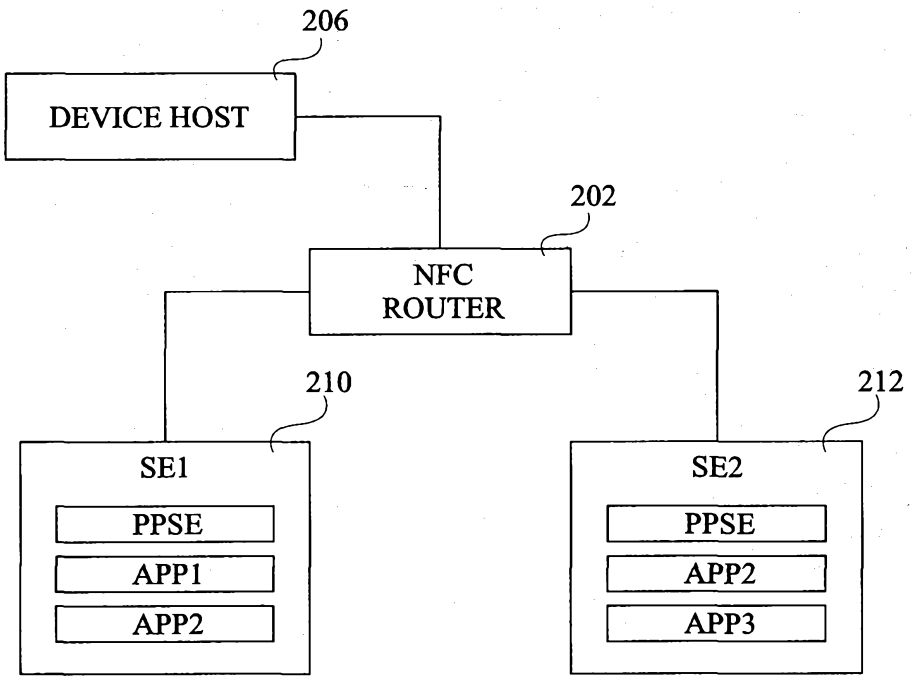
206
DEVICE HOST
202
NFC
ROUTER
210
212
SE1
PPSE
APP1
APP2
SE2
PPSE
APP2
APP3

Fig 3

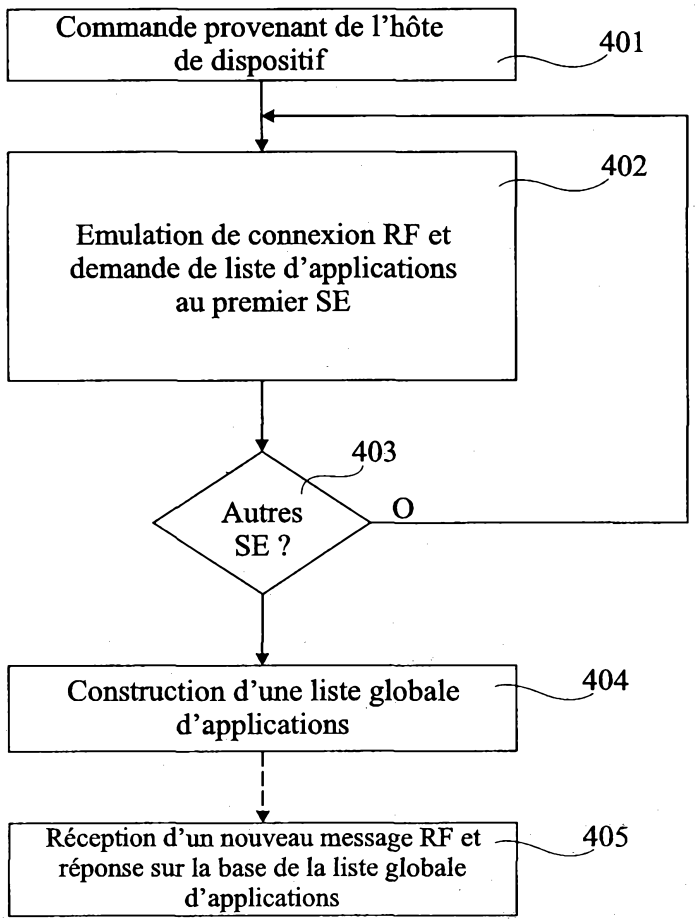
Commande provenant de l'hôte de dispositif
401
402
Emulation de connexion RF et demande de liste d'applications au premier SE
403
Autres SE ?
O
Construction d'une liste globale d'applications
404
Réception d'un nouveau message RF et réponse sur la base de la liste globale d'applications
405

Fig 4

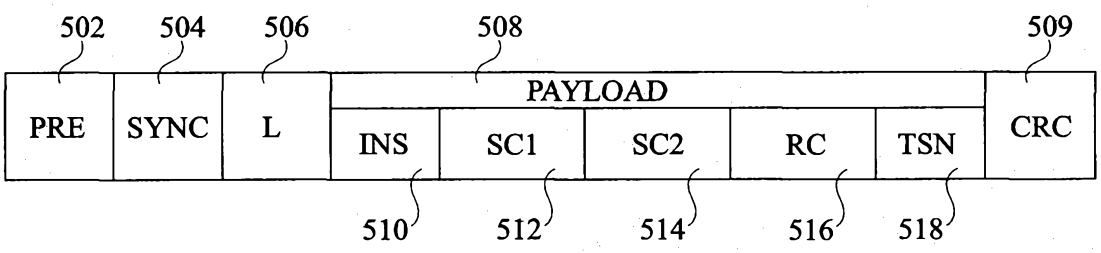

Fig 5

218

	TYPE OF ROUTING	AID/SC	TARGET	
ENTRY1	AID	A0000000031010	UICC	(VISA)
ENTRY2	FELICA	0002	UICC	(FELICA APPLICATION)
ENTRY3	AID	A0000000041010	eSE	(MASTERCARD)
ENTRY4	RF TYPE A	–	eSE	(MIFARE CLASSIC)
ENTRY5	FELICA	0003	eSE	(FELICA APPLICATION)

Fig 6

N° d'enregistrement national : 1557765 N° de publication : 3040226

RAPPORT DE RECHERCHE

articles L.612-14, L.612-17 et R.612-53 à 69 du code de la propriété intellectuelle

OBJET DU RAPPORT DE RECHERCHE

L'I.N.P.I. annexe à chaque brevet un "RAPPORT DE RECHERCHE" citant les éléments de l'état de la technique qui peuvent être pris en considération pour apprécier la brevetabilité de l'invention, au sens des articles L. 611-11 (nouveauté) et L. 611-14 (activité inventive) du code de la propriété intellectuelle. Ce rapport porte sur les revendications du brevet qui définissent l'objet de l'invention et délimitent l'étendue de la protection.

Après délivrance, l'I.N.P.I. peut, à la requête de toute personne intéressée, formuler un "AVIS DOCUMENTAIRE" sur la base des documents cités dans ce rapport de recherche et de tout autre document que le requérant souhaite voir prendre en considération.

CONDITIONS D'ÉTABLISSEMENT DU PRÉSENT RAPPORT DE RECHERCHE

- [x] Le demandeur a présenté des observations en réponse au rapport de recherche préliminaire.
- [ ] Le demandeur a maintenu les revendications.
- [x] Le demandeur a modifié les revendications.
- [ ] Le demandeur a modifié la description pour en éliminer les éléments qui n'étaient plus en concordance avec les nouvelles revendications.
- [ ] Les tiers ont présenté des observations après publication du rapport de recherche préliminaire.
- [ ] Un rapport de recherche préliminaire complémentaire a été établi.

DOCUMENTS CITÉS DANS LE PRÉSENT RAPPORT DE RECHERCHE

La répartition des documents entre les rubriques 1, 2 et 3 tient compte, le cas échéant, des revendications déposées en dernier lieu et/ou des observations présentées.

- [x] Les documents énumérés à la rubrique 1 ci-après sont susceptibles d'être pris en considération pour apprécier la brevetabilité de l'invention.
- [ ] Les documents énumérés à la rubrique 2 ci-après illustrent l'arrière-plan technologique général.
- [ ] Les documents énumérés à la rubrique 3 ci-après ont été cités en cours de procédure, mais leur pertinence dépend de la validité des priorités revendiquées.
- [ ] Aucun document n'a été cité en cours de procédure.

N° d'enregistrement national : 1557765 N° de publication : 3040226

1. ELEMENTS DE L'ETAT DE LA TECHNIQUE SUSCEPTIBLES D'ETRE PRIS EN CONSIDERATION POUR APPRECIER LA BREVETABILITE DE L'INVENTION

US 2015/020160 A1 (GONCALVES LOUIS-PHILIPPE [FR] ET AL)
15 janvier 2015 (2015-01-15)

EP 2 590 107 A1 (STMICROELECTRONICS APPLIC GMBH [DE])
8 mai 2013 (2013-05-08)

EP 2 600 639 A1 (BROADCOM CORP [US])
5 juin 2013 (2013-06-05)

US 2015/111495 A1 (VAN NIEUWENHUYZE OLIVIER [BE])
23 avril 2015 (2015-04-23)

2. ELEMENTS DE L'ETAT DE LA TECHNIQUE ILLUSTRANT L'ARRIERE-PLAN TECHNOLOGIQUE GENERAL

NEANT

3. ELEMENTS DE L'ETAT DE LA TECHNIQUE DONT LA PERTINENCE DEPEND DE LA VALIDITE DES PRIORITES

NEANT