



(10) Numéro de publication internationale
WO 2013/102708 A1

(43) Date de la publication internationale
11 juillet 2013 (11.07.2013)

W I P O I P C T

- (51) Classification internationale des brevets :
G06F 21/02 (2006.01) **G06Q 20/00** (2012.01)
H04L 29/06 (2006.01) **G06F 21/22** (2006.01)
G06F 21/00 (2013.01) **G06F 21/12** (2013.01)
- (21) Numéro de la demande internationale :
PCT/FR20 12/052289
- (22) Date de dépôt international :
9 octobre 2012 (09.10.2012)
- (25) Langue de dépôt : français
- (26) Langue de publication : français
- (30) Données relatives à la priorité :
125005 1 3 janvier 2012 (03.01.2012) FR
- (71) Déposant (*pour tous les États désignés sauf US*) : INSIDE
SECURE [FR/FR]; 41 Parc Club du Golf, F-13856 Aix-
en-Provence Cedex 3 (FR).
- (72) Inventeur; et
- (73) Déposant (*pour US seulement*) : CHEW, Gary [FR/FR];
12 Rue de la Verdière, Bât. 4, F-13090 Aix En Provence
(FR).
- (74) Mandataires : DE ROQUEMAUREL, Bruno et al; OM-
NIPAT, 24 Place des Martyrs de la Résistance, F-13100
Aix en Provence (FR).
- (81) États désignés (*sauf indication contraire, pour tout titre
de protection nationale disponible*) : AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY,
BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, ^{EST} IS, JP, KE, KG, KM, KN, KP,
KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD,
ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI,
NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU,
RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ,
TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA,
ZM, ZW.

[Suite sur la page suivante]

(54) Titre : METHOD FOR EXECUTING AN APPLICATION IN AN NFC DEVICE

(54) Titre : PROCEDE D'EXECUTION D'UNE APPLICATION DANS UN DISPOSITIF NFC

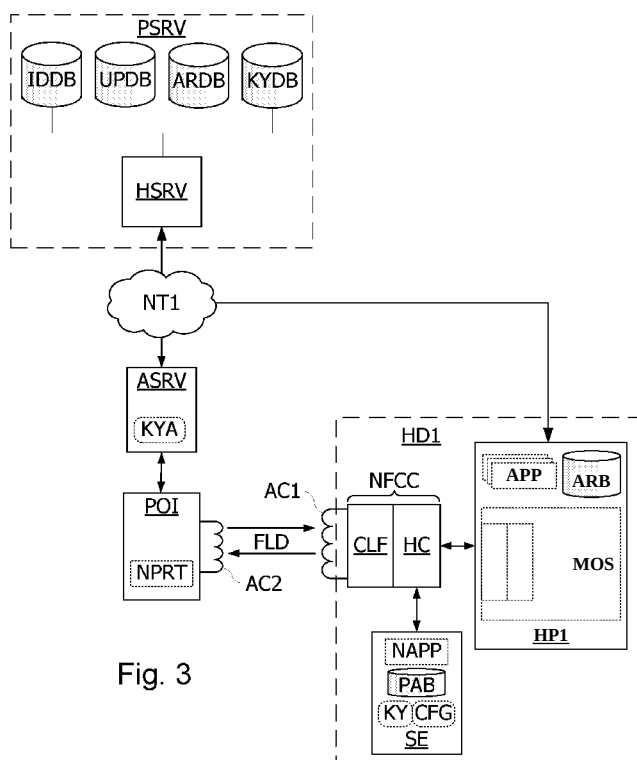


Fig. 3

(57) Abstract : The invention relates to a method for executing an application in an NFC device comprising steps during which: a contactless link is established between a first NFC device (HD1) and a second NFC device (POI), the first NFC device transmits, via the contactless link, an identifier stored by the first NFC device, the second NFC device transmits an application identifier via the contactless link, the second NFC device transmits the identifier of the first NFC device and the identifier of the application to an application server (ASRV), the application server transmits the identifier of the first NFC device and the identifier of the application to an authentication server (HSRV), the authentication server checks the identification data, and if the first NFC device and the application are identified, the authentication server authorises the two NFC devices to execute the application by transmitting, to the application server, an identifier of a user of the first NFC device corresponding to the identifier of the first NFC device.

(57) Abrégé :

[Suite sur la page suivante]

(84) **États désignés** (sauf indication contraire, pour tout titre de protection régionale disponible) : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,

SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— avec rapport de recherche internationale (Art. 21(3))

L'invention concerne un procédé d'exécution d'une application dans un dispositif NFC comprenant des étapes durant lesquelles : une liaison sans contact est établie entre un premier dispositif NFC (HD1) et un second dispositif NFC (POI), le premier dispositif NFC transmet par la liaison sans contact un identifiant mémorisé par le premier dispositif NFC, le second dispositif NFC transmet par la liaison sans contact un identifiant d'application, le second dispositif NFC transmet à un serveur d'application (ASRV) l'identifiant du premier dispositif NFC et l'identifiant de l'application, le serveur d'application transmet à un serveur d'authentification (HSRV) l'identifiant du premier dispositif NFC et l'identifiant de l'application, le serveur d'authentification vérifie les données d'identification, et si le premier dispositif NFC et l'application sont identifiés, le serveur d'authentification autorise les deux dispositifs NFC à exécuter l'application en transmettant au serveur d'application un identifiant d'un utilisateur du premier dispositif NFC correspondant à l'identifiant du premier dispositif NFC.

PROCEDE D'EXECUTION D'UNE APPLICATION DANS UN DISPOSITIF NFC

La présente invention concerne l'installation et l'exécution d'une application sécurisée dans un dispositif portable de type téléphone mobile ou équivalent.

La présente invention concerne également, mais non exclusivement,
5 la technologie NFC (Near Field Communication) ainsi que des architectures de dispositifs NFC ou "chipset NFC", c'est-à-dire des ensembles de puces comprenant au moins un composant NFC.

La technologie NFC est actuellement développée par un consortium industriel regroupé sous le nom de Forum NFC (<http://www.nfc-forum.org>).
10 La technologie NFC est dérivée de la technologie RFID (Radio Frequency Identification) et utilise des contrôleurs NFC présentant plusieurs modes de fonctionnement, notamment un mode lecteur ("Reader Mode"), un mode émulation de carte ("Card émulation") et un mode "peer-to-peer".

D'importants développements ont été réalisés ces dernières années
15 pour intégrer un contrôleur NFC dans des objets portables de type téléphone mobile ou équivalent (par exemple les assistants numériques personnels ou "PDA" équipés d'une fonction de téléphone mobile). Cette intégration vise notamment à doter de tels objets portables d'une application de paiement ou de contrôle d'accès (métro, autobus, etc.), et d'autres
20 applications de la technologie NFC comme la lecture d'étiquettes ou de cartes électroniques sans contact.

La figure 1 représente un dispositif NFC du type dispositif portable HD ("Handheld Device") tel un téléphone portable, un PDA (Assistant Numérique Personnel), etc. Le dispositif HD comprend un contrôleur NFC
25 référencé NFCC et au moins un processeur hôte processeur HP1, HP2 relié au contrôleur NFCC par un bus BS1, par exemple de type SWP ("Single Wire Protocol"). Un processeur hôte HP2 peut être une carte à circuit intégré désignée UICC ("Universal Integrated Circuit Card"), par exemple de type carte SIM (Subscriber Identity Module). Un processeur hôte HP1 peut
30 aussi être le processeur de bande de base ("Baseband") d'un téléphone mobile (soit le processeur en charge des communications téléphoniques). Dans ce cas, le processeur hôte HP1 peut être connecté au contrôleur

NFCC au moyen d'une liaison asynchrone BS2 gérée par des ports UART ("Universal Asynchronous Receiver Transiter"). Accessoirement, le processeur HP2 peut aussi être directement relié au processeur HP1 par un bus BS3 de type ISO 781 6.

5 Les ressources du contrôleur NFCC sont mises à la disposition du processeur hôte HP1 pour lui permettre de gérer des applications sans contact RAPI, CAPI. Le contrôleur NFCC comprend un contrôleur hôte HC et une interface sans contact CLF ("Contactless Front End Interface") équipée d'une bobine d'antenne AC1. En pratique, le contrôleur hôte HC et l'interface
10 CLF peuvent être réalisés sur une même puce de semi-conducteur, comme la puce MicroRead® commercialisée par la demanderesse, ou être formés de deux puces distinctes, comme les puces "PicoRead® Microcontroller" et "PicoRead® RF Interface" commercialisées par la demanderesse.

L'interface CLF du contrôleur NFCC peut généralement fonctionner
15 selon plusieurs technologies RF, par exemple de "Type A" telles que définies par ISO/IEC 14443 parties 2, 3 et 4, de "Type B" telle que définie par ISO/IEC 14443-2 avec un tramage normalisé ("standard framing") tel que défini par ISO/IEC 14443-3, et de "Type F" telle que définie par ISO 18092 en tant que mode passif à 212 et 424 ko/s (kilo octets par
20 seconde) ou par la norme industrielle japonaise JIS X 6319-4. Chaque technologie RF, ou protocole de communication sans contact, définit une fréquence d'émission du champ magnétique, une méthode de modulation du champ magnétique pour transmettre des données en mode actif, une méthode de modulation de charge pour transmettre des données en mode
25 passif, une méthode de codage des données, un format de trame de données, etc.

Des exemples d'application du dispositif NFC sont illustrés sur la figure 2 qui représente un dispositif portatif HD équipé du dispositif NFC de la figure 1, le dispositif HD prenant ici la forme d'un téléphone mobile. On
30 distingue des applications lecteur RAP ("Reader Applications") et des applications carte CAP ("Card Applications")

Applications lecteur (RAP)

Le contrôleur NFCC fonctionne comme un lecteur NFC pour conduire une transaction avec un circuit intégré sans contact CIC ("Contactless
35 Integrated Circuit"). Une application lecteur RAP, RAPI est exécutée par le processeur hôte HP1 (Cf. Fig. 1). Ce dernier place l'interface CLF dans un mode de fonctionnement actif où elle émet un champ magnétique FLD,

envoi des données par modulation du champ magnétique et reçoit des données par modulation de charge et couplage inductif. Ce type d'application peut être gratuit (par exemple lecture d'une étiquette électronique ou "tag" présente dans un abribus contenant les horaires des lignes de bus) et être exécutée par un processeur non sécurisé. Le processeur hôte HP1 peut dans ce cas être le processeur de bande de base du téléphone mobile. S'il s'agit d'une application payante, le processeur hôte exécutant l'application est de préférence un processeur sécurisé, par exemple un processeur de carte SIM, car l'accès au service nécessite une identification/authentification de l'abonné.

Applications carte (CAP)

Le principe de fonctionnement du mode émulation de carte est décrit par le brevet EP 1 327 222 (US 7 098 770) au nom de la demanderesse. Une application carte CAP, CAPI est exécutée par le processeur hôte HP1 (Cf. Fig. 1). Ce dernier place le contrôleur NFCC dans un mode de fonctionnement passif et forme avec le contrôleur NFCC, l'équivalent d'un circuit intégré sans contact, qui est vu par un lecteur RD comme une carte sans contact. Ainsi, le contrôleur NFCC n'émet pas de champ magnétique, reçoit des données en démodulant un champ magnétique FLD émis par le lecteur RD et émet des données par modulation de l'impédance de son circuit d'antenne AC1 (modulation de charge). Les applications concernées sont généralement des applications de paiement ou de contrôle d'accès payant (machine de paiement, entrée de métro, etc.). Le dispositif portatif HD est donc utilisé dans ce cas comme une carte à puce. Ce type d'application est le plus souvent sécurisé et le processeur hôte HP1, HP2 qui exécute le programme applicatif est alors un processeur sécurisé, par exemple un processeur de carte SIM, comportant des fonctions de cryptographie pour l'authentification de l'utilisateur et/ou l'authentification du dispositif portable vis-à-vis d'un terminal de transaction.

Diverses architectures de dispositifs NFC dédiées à la téléphonie ont été envisagées, certaines utilisant le processeur de la carte SIM pour gérer les applications NFC, d'autres prévoyant un second processeur sécurisé, les deux solutions pouvant être également combinées.

En raison notamment d'un nombre d'intervenants important et de la complexité des relations entre ces intervenants, la mise en œuvre d'une application sécurisée dans un dispositif NFC soulève des difficultés freinant le développement commercial des applications NFC sécurisées. En effet, le

dispositif portable, le processeur sécurisé et le contrôleur NFCC sont produits par des fabricants différents. Le processeur sécurisé (carte Sim) est généralement remis à un utilisateur final par un opérateur de réseau mobile, après avoir reçu des informations de sécurité telles que des identifiants, des clés secrètes et des certificats liés à l'utilisateur. Le dispositif portable peut être remis à l'utilisateur final par l'opérateur de réseau mobile ou une autre entité. L'application est réalisée par un développeur de logiciel. Si elle fait intervenir des transactions de paiement, l'application est certifiée par un organisme de certification lié à un organisme bancaire. Un composant logiciel d'une application, couramment appelé "applet", est installé de manière sécurisée dans le processeur hôte sécurisé et personnalisé avec des données d'identification de l'utilisateur et du dispositif portable et des clés de chiffrement propres à l'application et à l'utilisateur. L'utilisateur est également référencé de manière sécurisée auprès d'un organisme bancaire.

Une transaction de paiement fait intervenir un terminal de paiement qui est produit par encore un autre fabricant, et qui doit également avoir été certifié par un organisme de certification. L'utilisateur du terminal de paiement, un commerçant, doit également être référencé de manière sécurisée auprès d'un organisme bancaire. Les opérateurs de réseau mobiles sont généralement réticents à rendre les fonctions et données de sécurité des cartes SIM accessibles à d'autres intervenants tels que des fournisseurs d'applications sécurisées ou des services de paiement par carte. Il en résulte que l'installation d'une application nécessitant une authentification de l'utilisateur dans un dispositif portable soulève de nombreuses difficultés. Ces difficultés apparaissent à chaque fois qu'une application doit être installée notamment dans un processeur sécurisé du dispositif portable, et en particulier lorsqu'un utilisateur change de dispositif portable (téléphone mobile) et doit réinstaller les applications précédemment installées dans un ancien dispositif portable.

Par ailleurs, face à un faible nombre d'applications disponibles, les fabricants de téléphones mobiles ne voient pas l'intérêt d'augmenter le coût de leurs téléphones en y intégrant un contrôleur NFC et le cas échéant un processeur sécurisé supplémentaire.

Il peut être donc souhaitable de réaliser une architecture de déploiement d'applications NFC, qui ne nécessite pas la contribution

d'opérateurs de réseau mobile, tout en offrant si nécessaire un niveau de sécurité compatible avec les services de paiement et de contrôle d'accès payant. Il peut être également souhaitable que cette architecture ne nécessite pas la mise en œuvre d'un serveur centralisé de confiance pour assurer la gestion (émission, contrôle, révocation) de données secrètes attribuées à chaque dispositif mobile pour chaque application. Il peut être aussi souhaitable que chaque application NFC installée dans un dispositif portable ne soit pas attachée à un dispositif portable particulier, mais puisse être facilement activée dans un autre dispositif portable. Il peut être également souhaitable que le fournisseur d'une application puisse facilement permettre à un utilisateur d'accéder à l'application, en minimisant l'intervention de ce dernier, et ce sans avoir à faire intervenir l'opérateur de réseau mobile ou d'autres entités. Il peut être également souhaitable de garantir l'anonymat de l'utilisateur lorsqu'il exécute une application NFC, et en particulier d'empêcher un tiers d'établir un lien entre un dispositif NFC et l'identité de l'utilisateur du dispositif NFC.

Des modes de réalisation concernant un procédé d'exécution d'une application dans un dispositif NFC, le procédé comprenant des étapes durant lesquelles : une liaison sans contact est établie entre un premier dispositif NFC et un second dispositif NFC, le premier dispositif NFC transmet par la liaison sans contact un identifiant mémorisé par le premier dispositif NFC au second dispositif NFC, le second dispositif NFC transmet par la liaison sans contact un identifiant d'application au premier dispositif NFC, le second dispositif NFC transmet à un serveur d'application l'identifiant mémorisé par le premier dispositif NFC et l'identifiant d'application, le serveur d'application transmet à un serveur d'authentification l'identifiant mémorisé par le premier dispositif NFC et l'identifiant d'application, le serveur d'authentification vérifie à partir de l'identifiant mémorisé par le premier dispositif NFC que le premier dispositif NFC est autorisé à exécuter l'application identifiée par l'identifiant d'application, et si le premier dispositif NFC est autorisé à exécuter l'application, le serveur d'authentification autorise l'exécution de l'application en transmettant au serveur d'application un identifiant d'un utilisateur du premier dispositif NFC, correspondant à l'identifiant mémorisé par le premier dispositif NFC.

Selon un mode de réalisation, l'identifiant mémorisé par le premier dispositif NFC est modifié périodiquement par le serveur d'authentification qui tient à jour un lien entre l'identifiant de l'utilisateur et l'identifiant mémorisé par le premier dispositif NFC.

5 Selon un mode de réalisation, l'identifiant du premier dispositif NFC identifie un processeur sécurisé du premier dispositif NFC, le processeur sécurisé transmet par la liaison sans contact des premières données d'authentification permettant d'authentifier le processeur sécurisé du premier dispositif NFC, le second dispositif NFC transmet au serveur d'application
10 les premières données d'authentification, le serveur d'application transmet au serveur d'authentification les premières données d'authentification et des secondes données d'authentification permettant d'authentifier l'application correspondant à l'identifiant d'application, et le serveur d'authentification vérifie les données d'authentification, les deux dispositifs NFC étant
15 autorisés à exécuter l'application seulement si le processeur sécurisé et l'application sont authentifiés.

Selon un mode de réalisation, le premier dispositif NFC transmet au serveur d'authentification une requête d'installation d'application comprenant l'identifiant d'application d'une application à installer, et les premières
20 données d'authentification permettant d'authentifier le processeur sécurisé du premier dispositif NFC, le serveur d'authentification vérifie les premières données d'authentification, et si le processeur sécurisé est authentifié, transmet au premier dispositif NFC une adresse de téléchargement de l'application, et le premier dispositif NFC télécharge l'application à partir de
25 l'adresse de téléchargement reçue et installe l'application téléchargée.

Selon un mode de réalisation, à la suite de l'installation de l'application, le premier dispositif NFC informe le serveur d'authentification de l'installation de l'application en lui fournissant l'identifiant de l'application installée et les premières données d'authentification, et le serveur
30 d'authentification vérifie les premières données d'authentification, et si le processeur sécurisé est authentifié, le serveur d'authentification mémorise l'identifiant d'application en association avec l'identifiant du processeur sécurisé du premier dispositif NFC.

Selon un mode de réalisation, le serveur d'authentification ne
35 transmet pas au premier dispositif NFC une adresse de téléchargement de l'application si l'identifiant d'application est déjà mémorisé en association avec l'identifiant du processeur sécurisé du premier dispositif NFC.

Selon un mode de réalisation, le serveur d'authentification n'autorise pas l'exécution de l'application par les deux dispositifs NFC si l'identifiant d'application n'est pas mémorisé en association avec l'identifiant du processeur sécurisé du premier dispositif NFC.

5 Selon un mode de réalisation, les premières données d'authentification comprennent l'identifiant du processeur sécurisé et un premier cryptogramme calculé par le processeur sécurisé en appliquant à l'identifiant du processeur sécurisé, un calcul cryptographique utilisant une clé secrète mémorisée par le processeur sécurisé.

10 Selon un mode de réalisation, les secondes données d'authentification comprennent l'identifiant du processeur sécurisé, l'identifiant d'application et un second cryptogramme calculé par le serveur d'application en appliquant un calcul cryptographique à l'identifiant d'application, utilisant une clé secrète propre à l'application.

15 Selon un mode de réalisation, le second cryptogramme est calculé en appliquant le calcul cryptographique à l'identifiant d'application, et au premier cryptogramme.

 Selon un mode de réalisation, le premier et/ou le second cryptogrammes sont calculés à l'aide d'un algorithme de chiffrement symétrique utilisant une clé secrète, ou d'un algorithme de chiffrement asymétrique utilisant une clé privée, ou d'une fonction de hachage appliquée aux données à chiffrer et à la clé secrète.

20 Selon un mode de réalisation, la vérification de chacun des premier et second cryptogrammes est effectuée en recalculant le cryptogramme à partir des mêmes données et en utilisant une clé de chiffrement accessible au serveur d'authentification.

 Des modes de réalisation peuvent également concerner un système d'exécution d'une application sécurisée dans un dispositif NFC, comprenant : un premier dispositif NFC comprenant un composant NFC pour
30 établir une communication sans contact avec un autre dispositif NFC, et un processeur sécurisé connecté au composant NFC, un second dispositif NFC connecté à un serveur d'application pour exécuter une application avec autre dispositif NFC, un serveur d'authentification accessible au serveur d'application et au premier dispositif NFC, le système étant configuré pour
35 exécuter le procédé défini précédemment.

 Des modes de réalisation peuvent également concerner un ensemble d'un processeur sécurisé couplé à un composant NFC configuré pour établir

une communication sans contact avec un dispositif NFC, le processeur sécurisé comprenant un composant logiciel associé à un identifiant de processeur sécurisé, configuré pour : établir une communication sans contact avec un dispositif NFC par l'intermédiaire du contrôleur NFC, et
5 transmettre par la liaison sans contact l'identifiant, recevoir par la liaison sans contact un identifiant d'application, et transmettre par la liaison sans contact des données d'authentification du composant logiciel.

Selon un mode de réalisation, le composant logiciel est configuré pour vérifier si l'identifiant d'application reçu figure ou non dans une liste
10 d'applications mémorisée par le processeur sécurisé.

Selon un mode de réalisation, les données d'authentification comprennent l'identifiant du processeur sécurisé et un premier cryptogramme calculé par le processeur sécurisé en appliquant à l'identifiant du processeur sécurisé, un calcul cryptographique utilisant une clé secrète
15 mémorisée par le processeur sécurisé.

Selon un mode de réalisation, le premier cryptogramme est calculé par le processeur sécurisé à l'aide d'un algorithme de chiffrement symétrique utilisant une clé secrète, ou d'un algorithme de chiffrement asymétrique utilisant une clé privée, ou d'une fonction de hachage appliquée
20 aux données à chiffrer et à la clé secrète.

Des exemples de réalisation de l'invention seront décrits dans ce qui suit, à titre non limitatif en relation avec les figures jointes parmi lesquelles :

la figure 1 décrite précédemment représente schématiquement
25 l'architecture d'un dispositif NFC classique,

la figure 2 décrite précédemment représente schématiquement des exemples d'applications mises en œuvre dans le dispositif NFC,

la figure 3 représente schématiquement l'architecture d'un système de déploiement d'applications NFC,

30 les figures 4A à 4D représentent des tables d'une ou plusieurs bases de données utilisées par le système de déploiement,

la figure 5 représente des étapes d'activation d'une transaction impliquant l'exécution d'une application, entre un processeur hôte sécurisé du dispositif NFC et un lecteur NFC, selon un mode de réalisation,

35 la figure 6 représente des étapes d'installation et d'exécution d'une application dans un dispositif NFC, selon un mode de réalisation.

la figure 7 représente des étapes d'une procédure d'autorisation d'une transaction déclenchée par un dispositif d'interaction NFC durant l'exécution d'une application, selon un mode de réalisation,

La figure 3 représente l'architecture d'un système de déploiement d'application NFC. Le système de déploiement d'application comprend une pluralité de dispositifs portables NFC HD1 et de dispositifs d'interaction POI avec lesquels les dispositifs HD1 peuvent établir une communication sans contact NFC. Les dispositifs POI peuvent être des lecteurs sans contact NFC ou des circuits intégrés sans contact NFC. Les dispositifs POI sont chacun connectés ou connectables à un serveur d'application ASRV permettant l'exécution d'une transaction dans le cadre d'une application, avec un dispositif HD1 connecté au dispositif POI. Le dispositif POI comprend une antenne AC2 pour établir des communications sans contact NFC avec un dispositif NFC. Le dispositif POI peut être connecté au serveur ASRV soit directement, soit par l'intermédiaire d'un ou plusieurs réseaux de transmission de données.

Le dispositif HD1 comprend des processeurs hôte HP1, SE et un composant NFC référencé NFCC. Le processeur HP1 est par exemple un processeur de band de base ("baseband") de téléphone mobile, et le processeur hôte SE est un processeur sécurisé. Le composant NFCC comprend un contrôleur hôte HC connecté aux processeurs HP1 et SE et un circuit d'interface NFC référencé CLF connecté à un circuit d'antenne AC1. Le processeur HP1 comprend un système d'exploitation MOS et peut exécuter une ou plusieurs applications APP installées dans une mémoire du processeur HP1 (ou accessible au processeur HP1). Le processeur SE peut être le processeur d'une carte SIM ou un processeur distinct présentant au moins le même niveau de sécurité.

Selon un mode de réalisation, le système d'exploitation MOS comprend un logiciel pilote ONS permettant au processeur HP1 d'accéder à certaines fonctions du processeur SE par l'intermédiaire du contrôleur NFCC et de recevoir des notifications émises par le processeur SE. Le processeur HP1 comprend également une base de données d'applications ARB comprenant des références d'applications sécurisées APP installées dans la mémoire du processeur HP1. Le processeur SE comprend un composant logiciel, d'application appelé "applet NAPP", un identifiant du processeur SE

et un identifiant du composant NAPP, des clés de chiffrement KY, une liste PAB d'identifiants d'applications sécurisées installées dans le dispositif HD1, et des données de configuration du dispositif HD1 (type du dispositif, dénomination et version du système d'exploitation MOS, etc.). Les applications sécurisées APP peuvent être des applications de paiement, de contrôle d'accès, et plus généralement, des applications nécessitant une authentification. Le composant logiciel NAPP peut également mémoriser des informations de configuration CFG du dispositif HD1, ces informations comprenant notamment un type de dispositif et un numéro de version du système d'exploitation MOS. Le système d'exploitation MOS comprend également un logiciel de contrôle d'application à sécurisées NMNG communiquant avec le composant logiciel NAPP par l'intermédiaire du pilote ONS et du contrôleur NFCC. Le logiciel NMNG est configuré pour collecter des informations de configuration du dispositif HD1, et les transmettre au processeur SE. Le logiciel NMNG est lié de manière unique au composant logiciel NAPP de manière à masquer la présence du composant logiciel aux autres applications installées dans le processeur HP1. Ainsi, seul le logiciel NMNG est notifié lorsque le composant logiciel NAPP est sollicité par l'intermédiaire d'une liaison sans contact établie par le contrôleur NFCC, pour exécuter une application sécurisée. Le logiciel NMNG assure également une fonction de gestion de préférences de l'utilisateur du dispositif HD1.

Le système de déploiement d'application comprend un serveur de base de données HSRV donnant accès à une ou plusieurs bases de données IDDB, UPDB, ARDB, KYDB. Le logiciel NMNG assure également une fonction d'interface entre le serveur HSRV et le composant logiciel NAPP. Le serveur HSRV gère des identifiants de composants logiciels NAPP installés dans les processeurs SE des dispositifs HD1, des identifiants de fournisseurs d'application, et fournit des services d'authentification. Lors de sa fabrication, le processeur SE de chaque dispositif HD1 reçoit des identifiants uniques SEID et NID de processeur SE et de composant logiciel NAPP, des clés secrètes de chiffrement symétrique et/ou des clés publiques et privées de chiffrement asymétrique associées à un certificat. Le serveur HSRV assure des fonctions d'enregistrement et de radiation d'utilisateurs, de processeurs SE, de composants logiciels NAPP,

de fournisseurs d'application et d'applications. Chaque application est donc identifiée par un identifiant d'application unique.

Le contenu de la base ou des bases de données IDDB, UPDB, ARDB, KYDB est représenté sur les figures 4A à 4D. Sur la figure 4A, la
5 base de données IDDB est configurée pour établir une correspondance entre des identifiants SEID, NID du processeur SE et du composant logiciel NAPP de chaque processeur SE mis en service dans un dispositif HD1 . La base IDDB établit également une correspondance entre l'identifiant NID et un index de clé KIX permettant d'accéder aux clés de chiffrement associées,
10 mémorisées par le processeur SE. La base de données IDDB est donc complétée à chaque fois qu'un processeur SE est mis en service dans un dispositif HD1 . La base de données IDDB comprend également une table de correspondance entre des identifiants de composants logiciels NID installés dans un processeur SE et des identifiants d'application ARef, cette table
15 indique donc si une application ayant pour identifiant ARef est installée dans un dispositif HD1 dont le composant logiciel NAPP correspond à l'identifiant NID. La base IDDB est donc également mise à jour à chaque fois qu'une application est installée ou effacée d'un dispositif HD1 .

Sur la figure 4B, la base de données UPDB est configurée pour
20 établir une correspondance entre un identifiant NID attribué au composant logiciel NAPP et un identifiant d'utilisateur UID disposant du processeur SE installé dans le dispositif HD1 , ainsi qu'une correspondance entre l'identifiant UID et un index PRFX référençant des informations de profil UPRF relatives à l'utilisateur du dispositif HD1 . Comme un utilisateur peut
25 disposer de plusieurs processeurs SE, un identifiant d'utilisateur UID peut être associé dans la table UPDB à plusieurs identifiants NID de composants logiciels NAPP installés dans un processeur SE. La base de données UPDB est complétée lors de l'installation d'une première application dans un dispositif HD1 , et mise à jour à chaque fois que les informations de profil
30 d'un utilisateur sont modifiées.

Sur la figure 4C, la base de données ARDB est configurée pour établir une correspondance entre des identifiants de fournisseurs d'application PVID et des identifiants d'applications APID pour un type de dispositif HD1 , une correspondance entre chaque identifiant PVID et un
35 index de clé de chiffrement KIX permettant d'accéder à des clés de

chiffrement KIX propres au fournisseur d'application. La base ARDB établit également une correspondance entre chaque identifiant d'application APID et une référence DRF de type de dispositif HD1 dans lesquels l'application peut être installée et exécutée, et entre chaque référence DRF et une
5 adresse de téléchargement URL de l'application correspondant à l'identifiant APID. Chaque identifiant APID permet ainsi d'identifier chaque instance d'application adaptée à un type de dispositif HD1 et d'accéder à une adresse de téléchargement de l'instance d'application. La base ARDB est mise à jour à chaque enregistrement d'une nouvelle application prévue pour
10 un type de dispositif HD1 .

Sur la figure 4D, la base de données KYDB est configurée pour établir une correspondance entre chaque index de clé (de processeur SE ou de fournisseur d'application) et des clés de chiffrement. L'accès à la base de données KYDB peut être protégé par un serveur spécifique configuré pour
15 recevoir des index de clés KIX et des données à chiffrer ou à déchiffrer et pour fournir en réponse des cryptogrammes résultant du chiffrement ou déchiffrement des données fournies à l'aide des clés référencées par l'index de clé KIX fourni. La base KYDB est donc modifiée à chaque mise en service d'un nouveau processeur SE et à chaque enregistrement d'une
20 nouvelle application pour un type de dispositif HD1 .

Selon un mode de réalisation, chaque identifiant NID attribué à chaque utilisateur dans la base UPDB est modifié de temps en temps, par exemple périodiquement, par le serveur HSRV. Le serveur HSRV effectue cette modification également dans la base IDDB et transmet au dispositif
25 HD1 concerné le nouvel identifiant NID à utiliser, par exemple dans un message indiquant l'ancien et le nouvel identifiant NID. Chaque dispositif HD1 est configuré pour recevoir et traiter un tel message en transmettant l'ancien et le nouvel identifiant NID au processeur SE. Le processeur SE est configuré pour mémoriser le nouvel identifiant NID à la place de l'ancien
30 seulement si l'ancien identifiant reçu correspond à celui mémorisé par le processeur SE. Le processeur SE renvoie au serveur HSRV par l'intermédiaire du dispositif HD1 un message de compte rendu de mise à jour indiquant si la mise à jour de l'identifiant NID a été ou non effectuée. Le serveur HSRV peut répéter l'opération jusqu'à ce que la mise à jour soit
35 effectuée par le processeur SE. Bien entendu, les bases UPDB et IDDB ne

sont mises à jour que lorsque le processeur SE a envoyé au serveur HSRV un message de compte rendu indiquant qu'il a effectué la mise à jour.

La figure 5 représente une séquence d'étapes S1 à S13 déclenchée lorsqu'un dispositif HD1 est placé en communication sans contact avec un dispositif POI. Cette séquence est exécutée par le composant logiciel NAPP
5 installé dans le processeur SE du dispositif HD1 mis en communication avec le dispositif POI par l'intermédiaire du contrôleur NFFCC, par un logiciel de lecteur sans contact NPRT installé dans le dispositif POI et par le logiciel de gestion NMNG du processeur HP1 .

10 A l'étape S1, le logiciel NPRT envoie le cas échéant un message de sélection d'une application de paiement PPSE (Proximity Payment System Environment) au contrôleur NFCC. Le contrôleur NFCC retransmet le message PPSE au processeur SE. A l'étape S2, le processeur SE répond au message de sélection. A l'étape S3, le logiciel de lecteur NPRT envoie au
15 processeur SE un message de sélection du composant logiciel NAPP installé dans le processeur SE. En effet, plusieurs autres composants logiciels peuvent être installés dans le processeur SE. A l'étape S4, le composant logiciel NAPP répond au logiciel NPRT en lui fournissant son identifiant NID. A l'étape S5, le dispositif POI envoie un message
20 d'initialisation de transaction comprenant une information de type de transaction TTyp, un identifiant d'application APID, et des données de transaction. A l'étape S6, le composant logiciel NAPP vérifie si l'identifiant APID figure ou non dans la liste PAB d'identifiants d'applications installées dans le processeur HP1 . A l'étape S7, le composant logiciel NAPP répond
25 au message d'initialisation en indiquant si l'application APID est installée ou non dans le processeur HP1 . Quelle que soit la réponse du composant logiciel NAPP, le dispositif POI exécute l'étape S9 où il émet un ordre de lecture. Parallèlement à l'étape S8 le composant logiciel NAPP lance un calcul cryptographique pour obtenir un cryptogramme ED1 . A la suite de la
30 réception de l'ordre de lecture à l'étape S9, le composant logiciel NAPP émet en réponse à l'étape S10 le cryptogramme ED1 , ainsi que des données standard de transaction de paiement DATAI si l'application demandée est installée. Il est à noter que les étapes S1 à S9 sont conformes au standard de paiement par carte EMV (Europay, MasterCard
35 and Visa).

Durant les étapes S3 à S8, le composant logiciel NAPP émet une alerte à destination du logiciel de gestion NMNG installé dans le processeur HP1, pour l'informer qu'il a été sollicité par l'intermédiaire du contrôleur NFCC. A l'étape S11, le logiciel NMNG transmet au composant logiciel NAPP un message de demande de données. A l'étape S12, le composant logiciel NAPP transmet en réponse au logiciel NMNG le type de transaction TTyp reçu, l'identifiant d'application APID, le cryptogramme ED1 et une information d'état STS. A l'étape S13, le logiciel NMNG lance l'application dans le processeur HP1 ou une procédure d'installation de cette application si celle-ci n'est pas installée.

Le cryptogramme ED1 est par exemple calculé en appliquant une fonction cryptographique telle qu'une fonction de chiffrement symétrique comme AES (Advanced Encryption Standard) utilisant une clé mémorisée par le processeur SE, à l'identifiant NID, l'identifiant d'application APID, et éventuellement d'autres données. Le cryptogramme ED1 peut également être calculé à l'aide d'une fonction de hachage telle que SHA (Secure Hash Algorithm) ou MD5 (Message Digest 5) appliquées aux mêmes données, ainsi qu'à la clé mémorisée par le processeur SE. Le cryptogramme ED1 peut aussi être calculé par une fonction de chiffrement asymétrique utilisant une clé privée mémorisée par le processeur SE, la clé publique correspondante étant mémorisée dans la base KYDB. Les autres données utilisées dans le calcul du cryptogramme ED1 sont transmises avec celui-ci pour permettre par la suite sa vérification.

La figure 6 représente une séquence d'étapes S31 à S52 pouvant être exécutée à l'étape S13 par le dispositif HD1, et par les serveurs HSRV et ASRV. A l'étape S31, le logiciel NMNG du processeur HP1 détermine si l'application ayant pour identifiant APID est installée dans le dispositif HD1 en consultant la base de données ARB. Si l'application est déjà installée, le processeur HP1 exécute l'étape S48 où il peut être prévu de demander à l'utilisateur s'il accepte d'activer l'application. Si l'utilisateur accepte d'activer l'application, l'application est lancée à l'étape S49. Si l'application n'est pas installée dans le dispositif HD1, le processeur HP1 exécute l'étape S32 où il peut être prévu de demander à l'utilisateur s'il souhaite installer l'application dans le dispositif HD1. Si l'utilisateur accepte d'installer l'application, le processeur HP1 émet une requête de validation de téléchargement DLVal à

destination du serveur HSRV, cette requête étant accompagnée de l'identifiant d'un composant logiciel NID, du cryptogramme ED1 calculé à l'étape S7, et de l'identifiant d'application APID à télécharger. A l'étape S34, le serveur HSRV reçoit cette requête et vérifie le cryptogramme ED1 à l'aide
5 de l'identifiant NID et des informations contenues dans les bases de données IDDB, UPDB et KYDB, et vérifie l'existence de l'identifiant d'application dans la base ARDB. Le serveur HSRV vérifie également que l'application n'a pas déjà été installée dans le dispositif HD1 en vérifiant dans la base IDDB que l'identifiant NID n'est pas déjà lié à l'identifiant
10 d'application APID. La vérification de la liaison entre l'identifiant NID et l'identifiant d'application peut tenir compte du fait que l'application en cours d'installation est une mise à jour d'une application précédemment installée dans le dispositif HD1. Dans ce cas, l'installation est autorisée par le serveur HSRV. A l'étape S35, si toutes ces vérifications sont satisfaites, le serveur
15 HSRV exécute l'étape S36 où il détermine une adresse de téléchargement URL de l'application en accédant à la base ARDB à l'aide de l'identifiant APID. A l'étape S37, le serveur HSRV répond à la requête DLVal en fournissant le résultat des vérifications effectuées à l'étape S34. Si ces vérifications sont satisfaites, le serveur HSRV transmet également au
20 processeur HP1 l'adresse de téléchargement URL de l'application et éventuellement l'identifiant de l'application APID. Aux étapes S38 et S39 suivantes, le processeur HP1 reçoit ces informations du serveur HSRV, et si le téléchargement est autorisé par le serveur HSRV, procède au téléchargement de l'application en accédant à un serveur WSRV à l'adresse
25 URL reçue. A l'étape S40, le processeur HP1 lance l'installation de l'application en exécutant le fichier téléchargé à l'étape S39. A l'étape S42, le processeur HP1 demande au processeur SE par l'intermédiaire du composant logiciel NAPP d'introduire l'identifiant d'application APID dans la liste des identifiants d'applications PAB mémorisée par le processeur SE
30 pour chaque application de paiement. A l'étape S43, le processeur SE met à jour cette liste. Suite à l'étape S42, le processeur HP1 transmet au serveur HSRV une requête de validation d'installation d'application contenant l'identifiant NID, le cryptogramme ED1 et l'identifiant APID de l'application installée (étape S44). A l'étape S45 suivante, le serveur HSRV vérifie le
35 cryptogramme ED1. Si le cryptogramme ED1 est correct (étape S46), le

serveur HSRV mémorise que l'identifiant NID est lié à l'identifiant d'application APID dans la base IDDB (étape S47). A l'étape S48 suivante, si le cryptogramme ED1 est correct, le serveur HSRV transmet au processeur HP1 un message d'autorisation d'exécution de l'application
5 installée. A l'étape S49 suivante, le processeur HP1 met à jour la base de données ARB en y insérant l'identifiant APID de l'application installée, et lance l'exécution de l'application. Durant son exécution par le processeur HP1, l'application peut accéder au serveur de l'application ASRV ou un serveur associé (à l'étape S50), lequel peut demander au serveur HSRV des
10 informations de profil de l'utilisateur UPRF mémorisées dans la base UPDB, sur la base de l'identifiant NID, et demander à l'utilisateur le cas échéant de compléter ces informations, par exemple en affichant sur un écran d'affichage du dispositif HD1 un formulaire à remplir. Le formulaire affiché peut être pré rempli avec des informations relatives à l'utilisateur, figurant
15 déjà dans la base UPDB. Les informations de profil saisies par l'utilisateur peuvent être transmises par le processeur HP1 à un serveur lié à l'application, comme le serveur ASRV ou le serveur WSRV, qui lui-même les retransmet au serveur HSRV pour mettre à jour la base de données UPDB (étape S51). Durant l'exécution de l'application, le serveur ASRV peut
20 exécuter une transaction classique de paiement en accédant à un réseau bancaire sur la base d'informations d'identification de l'utilisateur obtenues à partir de l'identifiant NID dans la base UPDB.

Il peut être mis à disposition de l'utilisateur des procédures de blocage/déblocage d'une application, et de désinstallation d'une application.
25 Ces procédures se déroulent d'une manière analogue aux étapes S33 à S37, l'étape S33 étant remplacée par l'émission d'une requête correspondante de blocage, déblocage ou de désinstallation, et l'étape S36 étant remplacée par une étape d'exécution de la requête. A cet effet, il peut être prévu un indicateur d'état de blocage qui peut être prévu à chaque ligne
30 de la table de la base IDDB associant un identifiant d'application APID à un identifiant NID de composant logiciel NAPP. S'il s'agit d'une requête de blocage ou de déblocage d'application, le serveur HSRV peut mettre à jour l'indicateur d'état correspondant aux identifiants d'application APID et de composant logiciel NID reçus du processeur HP1. Cet indicateur d'état peut
35 être testé avant que le processeur HP1 exécute l'application à l'étape S49.

S'il s'agit d'une requête de désinstallation, le serveur HSRV peut supprimer la ligne de cette table associant les identifiants de composant logiciel et d'application reçus du processeur HP1. Bien entendu, les opérations de blocage/déblocage et de désinstallation d'applications ne sont effectuées qu'après vérification par le serveur HSRV du cryptogramme ED1 fourni par le processeur HP1, et de l'existence d'un lien entre les identifiants NID et APID dans la base IDDB.

Chaque élément de liste PAB mémorisée dans le processeur SE peut être associé à un numéro de priorité et à un indicateur de blocage, accessibles par une commande de configuration mise à disposition de l'utilisateur par l'intermédiaire du processeur HP1. De cette manière, si plusieurs applications de paiement enregistrées dans la liste PAD sont compatibles avec l'identifiant APID transmis par le dispositif POI à l'étape S5, le composant logiciel NAPP active l'application de paiement non bloquée ayant le plus grand numéro de priorité.

La figure 7 représente une séquence d'étapes S61 à S70 pouvant être déclenchée par le dispositif POI au lancement et lors de l'exécution d'une application à la suite des étapes S9 et S49 ou d'une application de paiement lancée par l'application activée à l'étape S49. Cette séquence d'étapes est exécutée par le dispositif POI, le serveur d'application ASRV et le serveur HSRV. A l'étape S61, le dispositif POI transmet au serveur ASRV une requête de transaction TTReq contenant des données relatives à l'application AppData, l'identifiant du composant logiciel NID reçu à l'étape S4, et le cryptogramme ED1 reçu à l'étape S9. A l'étape S62, le serveur ASRV reçoit cette requête et lance un calcul cryptographique pour obtenir un cryptogramme ED2 notamment à partir de l'identifiant d'application APID. A l'étape S63, le serveur ASRV émet à destination du serveur HSRV une requête d'authentification AuthReq contenant l'identifiant du composant logiciel NID, les cryptogrammes ED1 et ED2 et l'identifiant de l'application APID. A l'étape S64, le serveur HSRV vérifie l'existence de l'identifiant NID dans la base de données IDDB et vérifie le cryptogramme ED1. A l'étape S65, le serveur HSRV vérifie l'existence de l'identifiant d'application APID dans la base ARDB, et vérifie le cryptogramme ED2. A l'étape S66, le serveur HSRV vérifie dans la base de données IDDB que l'application est liée à l'identifiant NID de processeur SE du dispositif HD1 connecté au

dispositif POI. A l'étape S67, le serveur HSRV émet à destination du serveur ASRV un message de réponse d'authentification AuthRep indiquant le succès ou l'échec de l'authentification, c'est-à-dire si les cryptogrammes ED1, ED2 reçus sont authentiques, et si l'application ayant l'identifiant APID est bien liée à l'identifiant NID du dispositif HD1 connecté au dispositif POI. Si l'authentification a réussi, le serveur HSRV transmet également si nécessaire, l'identifiant de l'utilisateur UID au serveur ASRV pour permettre à ce dernier d'effectuer une transaction sur la base de l'identité de l'utilisateur. A l'étape S68, le serveur ASRV teste le message de réponse d'authentification et si l'authentification a réussi, il exécute les étapes S69 et S70 où il exécute la transaction correspondant à l'application et à l'utilisateur et il transmet au dispositif POI un message de réponse de transaction TTRep à la requête transmise à l'étape S61. Le serveur ASRV peut ainsi être assuré de l'authenticité des identifiants NID et APID.

Le cryptogramme ED2 peut être calculé (à l'étape 62) en appliquant la fonction utilisée pour calculer le cryptogramme ED1, à l'identifiant d'application APID, et éventuellement au cryptogramme ED1 et à d'autres données telles qu'un nombre généré aléatoirement. Les autres données utilisées dans le calcul du cryptogramme ED2, et en particulier le nombre aléatoire sont transmis avec le cryptogramme ED2 pour permettre sa vérification par le serveur HSRV. Si les cryptogrammes sont calculés à l'aide d'une fonction de chiffrement symétrique ou une fonction de hachage, utilisant une clé secrète, les cryptogrammes ED1, ED2 peuvent être vérifiés en les recalculant à l'aide des mêmes clés secrètes et des même données utilisées pour leur premier calcul. Les données secrètes sont mémorisées dans la base KYDB en association avec les identifiants NID, APID. Les données éventuellement utilisées pour le calcul du cryptogramme ED1 peuvent se trouver dans la base IDDB en association avec l'identifiant NID. Les données éventuellement utilisées pour le calcul du cryptogramme ED2 peuvent se trouver dans la base ARDB en association avec l'identifiant APID. Si les cryptogrammes ED1, ED2 ont été calculés à l'aide d'un algorithme de chiffrement asymétrique, ils peuvent être vérifiés en leur appliquant le même algorithme de chiffrement utilisant des clés publiques mémorisées dans la base KYDB, correspondant aux clés secrètes utilisées pour leur calcul.

Il est à noter que l'identifiant de l'utilisateur UID n'est jamais transmis ou reçu par le dispositif NFC HD1, mais seulement par les liaisons entre les serveurs ASRV, HSRV qui peuvent être sécurisées. L'anonymat de l'utilisateur peut ainsi être préservé, sachant que l'identifiant NID est
5 insuffisant pour identifier un utilisateur et que l'identifiant SEID du processeur SE n'est jamais transmis lors de l'exécution d'une application.

Bien entendu, le serveur d'authentification HSRV peut en réalité être réalisé par plusieurs serveurs connectés entre eux. Ainsi, la base de clés de chiffrement KYDB peut être accessible par l'intermédiaire d'un serveur
10 spécifique. Les données de chacune des bases IDDB, UPDB, ARDB et KYDB peuvent également être réparties dans plusieurs bases de données accessibles par des serveurs distincts.

Grâce à ces dispositions, l'installation d'une nouvelle application ne nécessite pas d'installer un composant logiciel dans un processeur sécurisé
15 SE du dispositif NFC HD1. Le processeur sécurisé SE est personnalisé une seule fois et pour toutes les applications NFC susceptibles d'être exécutées par le processeur HP1, en recevant le composant NAPP associé à un identifiant unique NID et une ou plusieurs clés secrètes associées. Comme un seul composant logiciel NAPP peut être installé dans le processeur SE,
20 l'identifiant NID peut être utilisé pour identifier le processeur SE. L'installation du composant NAPP dans le processeur SE n'empêche nullement l'installation ou l'exécution d'autres composants logiciels dans le processeur SE. Comme le lien entre une application et le dispositif HD1 d'un utilisateur est établi à l'extérieur du dispositif HD1, à savoir par les bases de
25 données IDDB, UPDB, ARDB, ce lien peut être facilement rétabli pour et à partir d'un autre dispositif NFC, en cas de perte, vol ou échange du dispositif HD1. Les cryptogrammes ED1 et ED2 permettent d'authentifier le processeur SE et l'application. Par ailleurs, il convient de remarquer que les séquences d'étapes décrites précédemment ne font pas intervenir un
30 opérateur de réseau mobile, sauf éventuellement pour établir une communication entre le dispositif HD1 (du type téléphone mobile) et un serveur de téléchargement d'application WSRV.

Il apparaîtra clairement à l'homme de l'art que la présente invention est susceptible de diverses variantes de réalisation et diverses applications.
35 En particulier, l'invention n'est pas limitée à la mise en œuvre d'applications

sécurisées. Ainsi, la génération, la transmission et la vérification de l'un et/ou l'autre des cryptogrammes ED1, ED2 n'est pas nécessaire pour la mise en œuvre de l'invention.

L'invention n'est pas non plus limitée aux dispositifs NFC dans
5 lesquels le contrôleur NFCC est connecté au processeur HP1. En effet, le contrôleur NFCC et le processeur sécurisé SE peuvent être intégrés dans une puce associée à un téléphone mobile par un moyen mécanique quelconque (sticker, housse de téléphone mobile). Par exemple, sur la figure 5, la transmission des données nécessaires à l'exécution d'une
10 application par le processeur HP1 peuvent être transmises au processeur HP1 par l'intermédiaire du serveur ASRV connecté au dispositif POI. L'application dans le processeur HP1 peut également être lancée manuellement par l'utilisateur.

Les étapes de téléchargement et d'installation d'une application dans
15 le processeur HP1 ne sont pas non plus nécessaires. Ces opérations peuvent en effet être effectuées lors de l'installation du système d'exploitation MOS dans le processeur HP1. Le dispositif NFC HD1 peut ainsi être livré à un utilisateur avec un certain nombre d'applications déjà installées dans le processeur HP1.

20 Par ailleurs, selon les applications ("Reader Applications, "Card Applications"), le dispositif HD1 peut établir une liaison sans contact avec un dispositif externe NFC (POI) en mode carte, ou en mode lecteur, ou encore en mode "peer-to-peer". Ainsi, l'exécution de la séquence d'étapes de la figure 6, n'est pas nécessairement effectuée de manière synchrone. En effet,
25 notamment dans le cas où le dispositif POI est un circuit intégré sans contact, les étapes S61 et S70 peuvent être effectuées de manière différées lorsque le dispositif POI peut établir une communication avec le serveur d'application ASRV.

REVENDEICATIONS

1. Procédé d'exécution d'une application dans un dispositif NFC, le procédé comprenant des étapes durant lesquelles :

une liaison sans contact est établie entre un premier dispositif NFC (HD1) et un second dispositif NFC (POI),

5 le premier dispositif NFC transmet par la liaison sans contact un identifiant (NID) mémorisé par le premier dispositif NFC au second dispositif NFC,

le second dispositif NFC transmet par la liaison sans contact un identifiant d'application (APID) au premier dispositif NFC,

10 le second dispositif NFC transmet à un serveur d'application (ASRV) l'identifiant mémorisé par le premier dispositif NFC et l'identifiant d'application,

le serveur d'application transmet à un serveur d'authentification (HSRV) l'identifiant mémorisé par le premier dispositif NFC et l'identifiant d'application,

15 le serveur d'authentification vérifie à partir de l'identifiant mémorisé par le premier dispositif NFC que le premier dispositif NFC est autorisé à exécuter l'application identifiée par l'identifiant d'application, et

si le premier dispositif NFC est autorisé à exécuter l'application, le serveur d'authentification autorise l'exécution de l'application en transmettant au serveur d'application un identifiant (UID) d'un utilisateur du premier dispositif NFC, correspondant à l'identifiant mémorisé par le premier dispositif NFC.

25 2. Procédé selon la revendication 1, dans lequel l'identifiant (NID) mémorisé par le premier dispositif NFC (HD1) est modifié périodiquement par le serveur d'authentification (HSRV) qui tient à jour un lien entre l'identifiant de l'utilisateur (UID) et l'identifiant mémorisé par le premier dispositif NFC.

30

3. Procédé selon la revendication 1 ou 2, dans lequel :

l'identifiant (NID) du premier dispositif NFC (HD1) identifie un processeur sécurisé (SE) du premier dispositif NFC,

le processeur sécurisé transmet par la liaison sans contact des premières données d'authentification (ED1) permettant d'authentifier le processeur sécurisé du premier dispositif NFC,

le second dispositif NFC transmet au serveur d'application (ASRV)
5 les premières données d'authentification,

le serveur d'application transmet au serveur d'authentification (HSRV) les premières données d'authentification et des secondes données d'authentification (ED2) permettant d'authentifier l'application correspondant à l'identifiant d'application, et

10 le serveur d'authentification vérifie les données d'authentification, les deux dispositifs NFC étant autorisés à exécuter l'application seulement si le processeur sécurisé et l'application sont authentifiés.

4. Procédé selon la revendication 3, dans lequel :

15 le premier dispositif NFC transmet au serveur d'authentification (HSRV) une requête d'installation d'application comprenant l'identifiant d'application (APID) d'une application à installer, et les premières données d'authentification permettant d'authentifier le processeur sécurisé (SE) du premier dispositif NFC,

20 le serveur d'authentification vérifie les premières données d'authentification, et si le processeur sécurisé est authentifié, transmet au premier dispositif NFC une adresse de téléchargement (URL) de l'application, et

le premier dispositif NFC télécharge l'application à partir de l'adresse
25 de téléchargement reçue et installe l'application téléchargée.

5. Procédé selon la revendication 4, dans lequel, à la suite de l'installation de l'application, le premier dispositif NFC (HD1) informe le serveur d'authentification (HSRV) de l'installation de l'application en lui
30 fournissant l'identifiant (APID) de l'application installée et les premières données d'authentification, et

le serveur d'authentification vérifie les premières données d'authentification, et si le processeur sécurisé (SE) est authentifié, le serveur d'authentification mémorise l'identifiant d'application en association avec
35 l'identifiant du processeur sécurisé (SE) du premier dispositif NFC.

6. Procédé selon la revendication 5, dans lequel le serveur d'authentification (HSRV) ne transmet pas au premier dispositif NFC (HD1) une adresse de téléchargement de l'application si l'identifiant d'application (APID) est déjà mémorisé en association avec l'identifiant (NID) du processeur sécurisé (SE) du premier dispositif NFC.

7. Procédé selon la revendication 5 ou 6, dans lequel le serveur d'authentification (HSRV) n'autorise pas l'exécution de l'application par les deux dispositifs NFC (HD1, POI) si l'identifiant d'application (APID) n'est pas mémorisé en association avec l'identifiant (NID) du processeur sécurisé (SE) du premier dispositif NFC.

8. Procédé selon l'une des revendications 1 à 7, dans lequel les premières données d'authentification comprennent l'identifiant du processeur sécurisé (NID) et un premier cryptogramme (ED1) calculé par le processeur sécurisé (SE) en appliquant à l'identifiant du processeur sécurisé (NID), un calcul cryptographique utilisant une clé secrète (KY) mémorisée par le processeur sécurisé.

9. Procédé selon l'une des revendications 1 à 8, dans lequel les secondes données d'authentification comprennent l'identifiant du processeur sécurisé (NID), l'identifiant d'application (APID) et un second cryptogramme (ED2) calculé par le serveur d'application en appliquant un calcul cryptographique à l'identifiant d'application (APID), utilisant une clé secrète (KYA) propre à l'application.

10. Procédé selon la revendication 9, dans lequel le second cryptogramme (ED2) est calculé en appliquant le calcul cryptographique à l'identifiant d'application (APID), et au premier cryptogramme (ED1).

11. Procédé selon l'une des revendications 1 à 10, dans lequel le premier et/ou le second cryptogrammes (ED1, ED2) sont calculés à l'aide d'un algorithme de chiffrement symétrique utilisant une clé secrète, ou d'un

algorithme de chiffrement asymétrique utilisant une clé privée, ou d'une fonction de hachage appliquée aux données à chiffrer et à la clé secrète.

12. Procédé selon l'une des revendications 1 à 11, dans lequel la
5 vérification de chacun des premier et second cryptogrammes (ED1 , ED2) est effectuée en recalculant le cryptogramme à partir des mêmes données et en utilisant une clé de chiffrement accessible au serveur d'authentification.

13. Système d'exécution d'une application sécurisée dans un
10 dispositif NFC, comprenant :

un premier dispositif NFC (HD1) comprenant un composant NFC (NFCC) pour établir une communication sans contact avec un autre dispositif NFC, et un processeur sécurisé (SE) connecté au composant NFC,
un second dispositif NFC (POI) connecté à un serveur d'application
15 (ASRV) pour exécuter une application avec autre dispositif NFC,

caractérisé en ce qu'il comprend un serveur d'authentification (HSRV) accessible au serveur d'application (ASRV) et au premier dispositif NFC (HD1), le système étant configuré pour exécuter le procédé selon l'une des revendications 1 à 10.

20

14. Ensemble d'un processeur sécurisé couplé à un composant NFC (NFCC) configuré pour établir une communication sans contact avec un dispositif NFC (POI),

caractérisé en ce que le processeur sécurisé (SE) comprend un
25 composant logiciel (NAPP) associé à un identifiant (NID) de processeur sécurisé, configuré pour :

établir une communication sans contact avec un dispositif NFC par l'intermédiaire du contrôleur NFC, et transmettre par la liaison sans contact l'identifiant,

30 recevoir par la liaison sans contact un identifiant d'application (APID),
et

transmettre par la liaison sans contact des données d'authentification du composant logiciel.

15. Ensemble selon la revendication 14, dans lequel le composant logiciel est configuré pour vérifier si l'identifiant d'application (APID) reçu figure ou non dans une liste d'applications mémorisée par le processeur sécurisé.

5

16. Ensemble selon la revendication 14 ou 15, dans lequel les données d'authentification comprennent l'identifiant du processeur sécurisé (NID) et un premier cryptogramme (ED1) calculé par le processeur sécurisé (SE) en appliquant à l'identifiant du processeur sécurisé (NID), un calcul
10 cryptographique utilisant une clé secrète (KY) mémorisée par le processeur sécurisé.

17. Ensemble selon la revendication 16, dans lequel le premier
15 cryptogramme (ED1) est calculé par le processeur sécurisé (SE) à l'aide d'un algorithme de chiffrement symétrique utilisant une clé secrète, ou d'un algorithme de chiffrement asymétrique utilisant une clé privée, ou d'une fonction de hachage appliquée aux données à chiffrer et à la clé secrète.

1/6

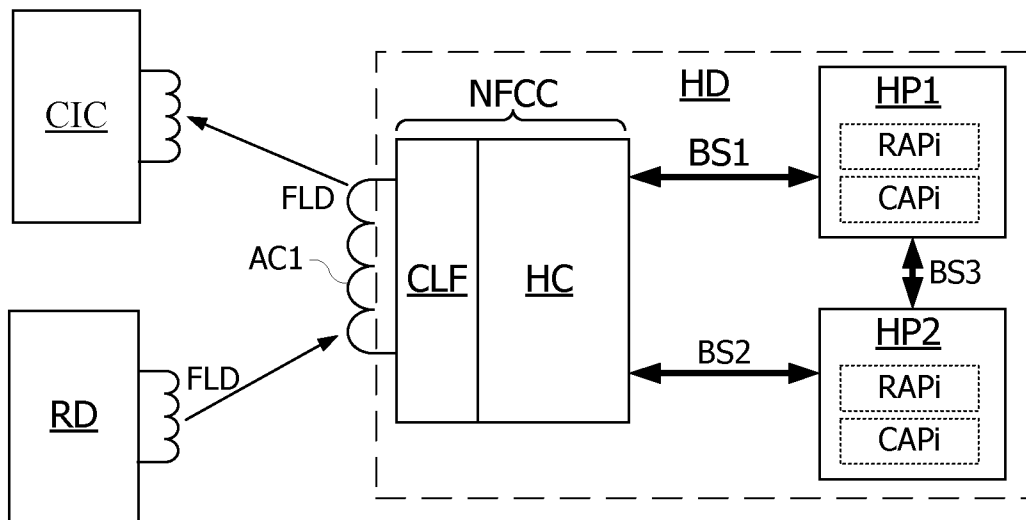


Fig. 1

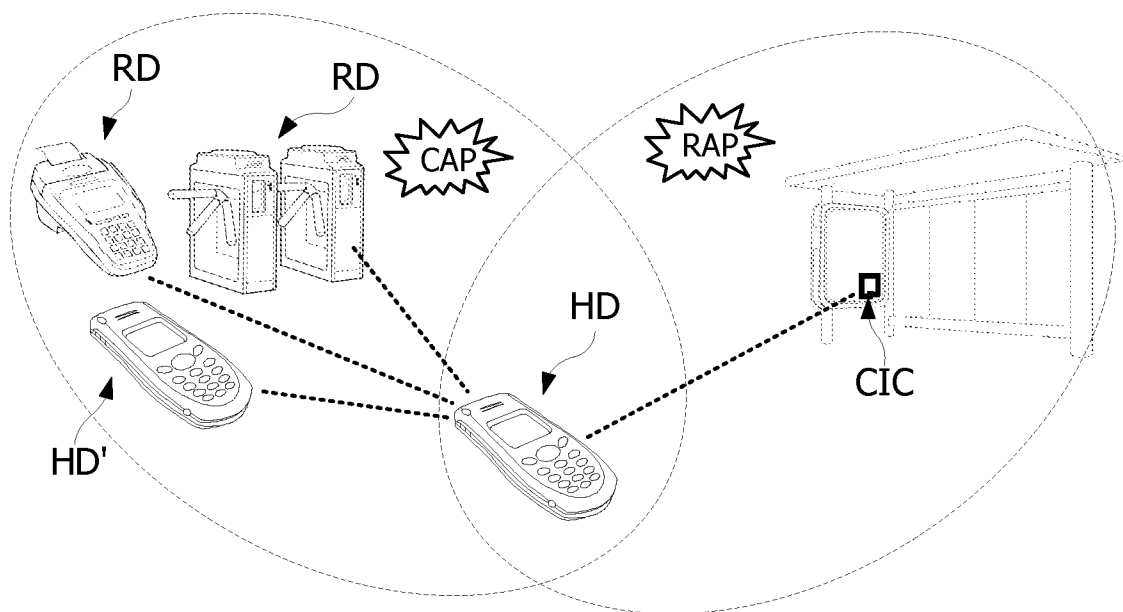


Fig. 2

2/6

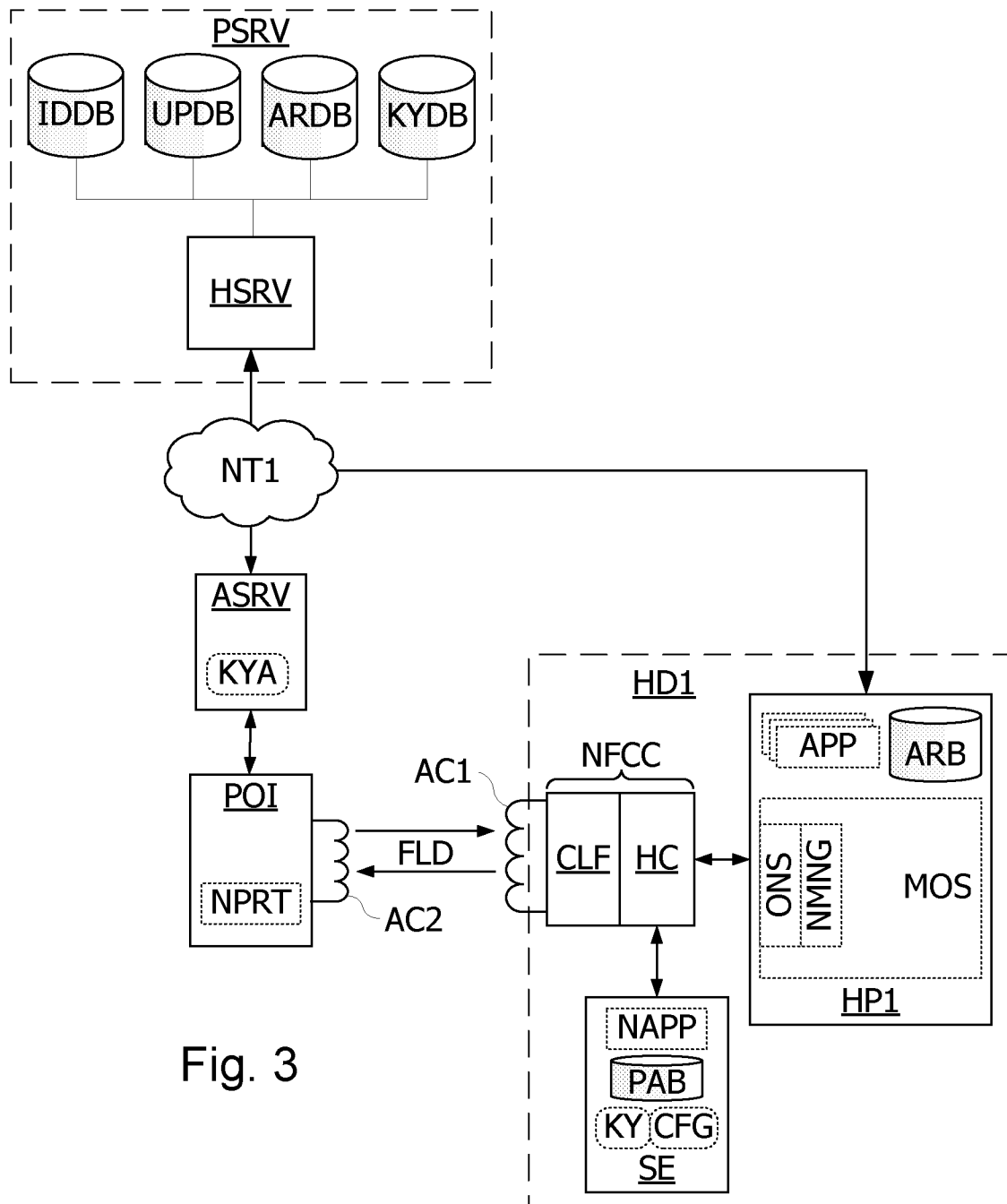


Fig. 3

IDDB

SEID	UID
...	...
...	...
...	...
...	...

UID	KIX	UID	APID
...	...	...	...
...	...	...	...
...	...	...	...
...	...	...	...

Fig. 4A

UPDB

NID	UID
...	...
...	...
...	...
...	...

UID	PRFX	UPRF
...	...	...
...	...	...
...	...	...
...	...	...

Fig. 4B

ARDB

PVID	APID
...	...
...	...
...	...
...	...

APID	DRF	URL
...	...	...
...	...	...
...	...	...
...	...	...

PVID	KIX
...	...
...	...
...	...
...	...

Fig. 4C

KYDB

KIX	KEY
...	...
...	...
...	...
...	...

Fig. 4D

4/6

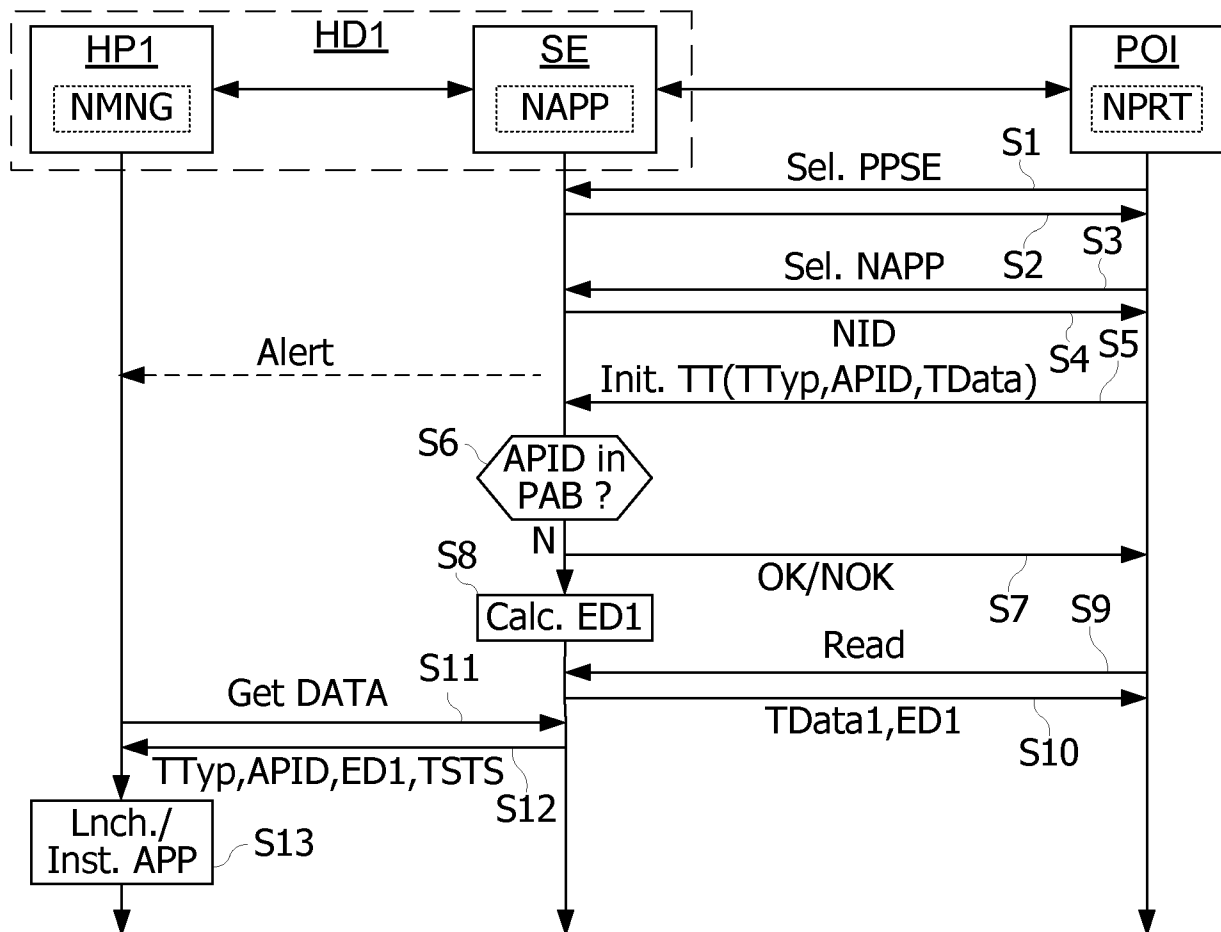


Fig. 5

5/6

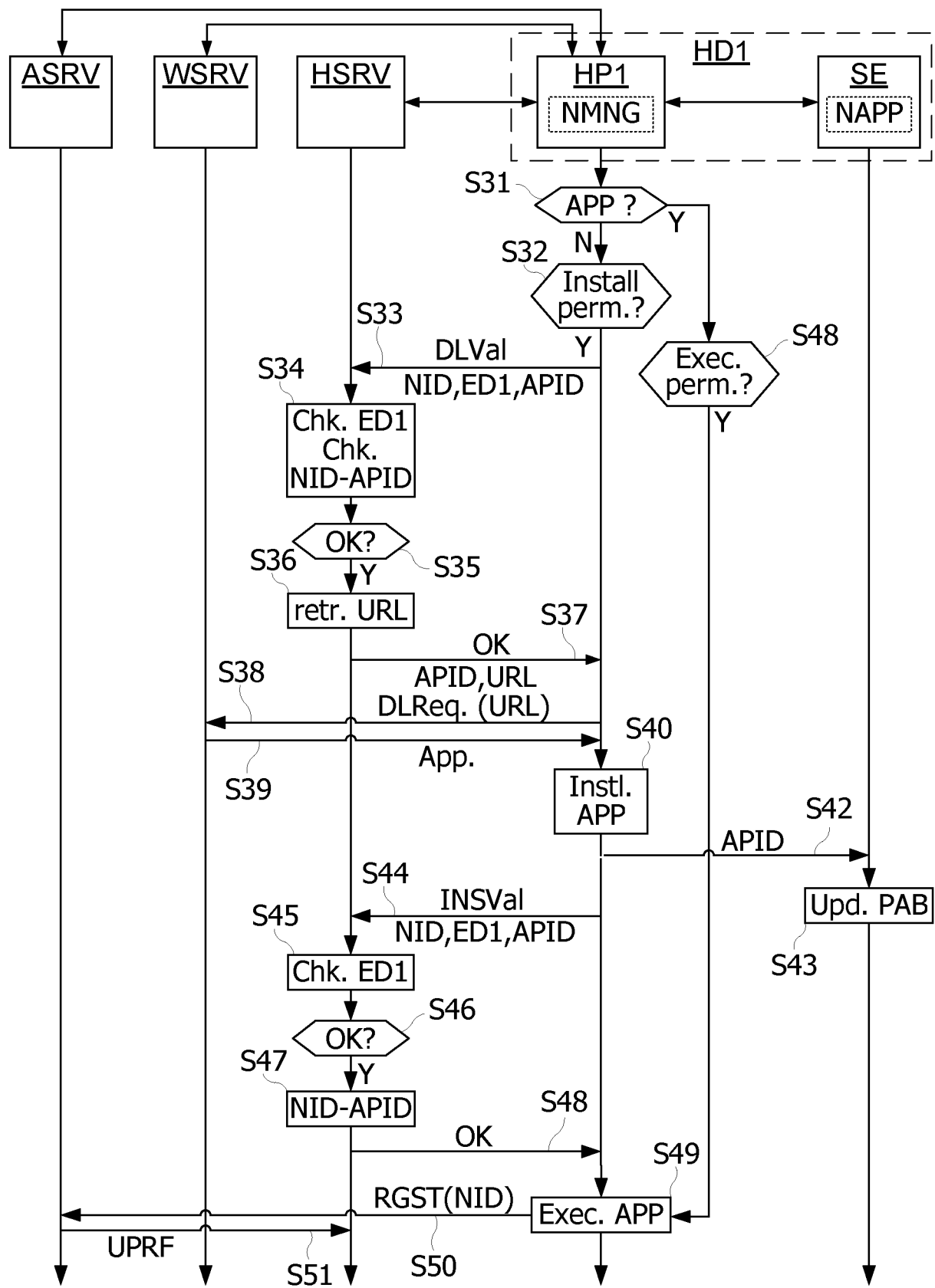


Fig. 6

6/6

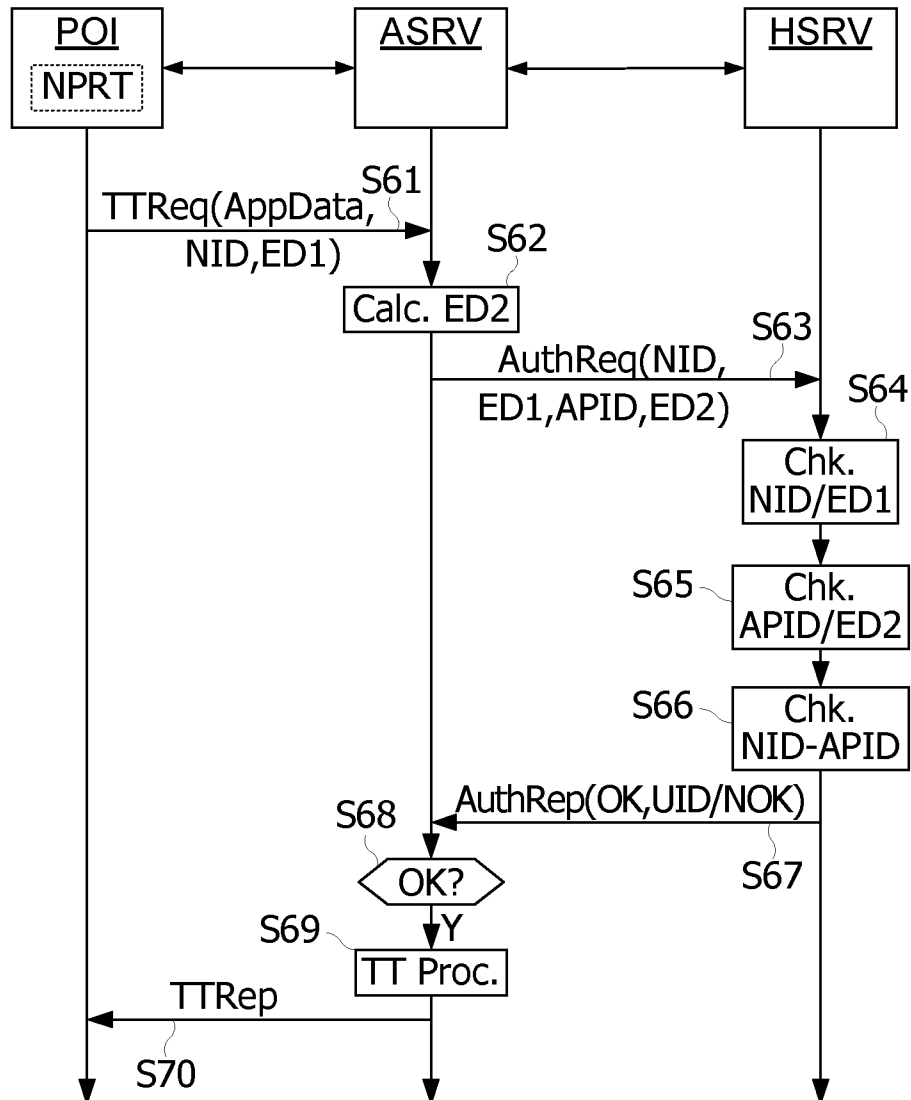


Fig. 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2012/052289

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F21/02 H04L29/06 G06F21/00 G06Q20/00 G06F21/22
G06F21/12

ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification System followed by classification symbol)

H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	FR 2 935 510 A1 (OBERTHUR TECHNOLOGIES [FR]) 5 March 2010 (2010-03-05) page 6, line 30 - page 19, line 14; figures 1-6 -----	1-17



Further documents are listed in the continuation of Box C.



See patent family annex.

* Spécial catégories de cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

29 November 2012

Date of mailing of the international search report

12/12/2012

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Savvides, George

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/FR2012/052289

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2935510	AI	05-03-2010	EP 2160002 AI 03-03-2010
			FR 2935510 AI 05-03-2010
			JP 2010061659 A 18-03-2010
			US 2010058463 AI 04-03-2010

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2012/052289

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06F21/02 H04L29/06 G06F21/00 G06Q20/00 G06F21/22
G06F21/12

ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04L G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal , WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	FR 2 935 510 A1 (OBERTHUR TECHNOLOGIES [FR]) 5 mars 2010 (2010-03-05) page 6, ligne 30 - page 19, ligne 14; figures 1-6 -----	1-17



Voir la suite du cadre C pour la fin de la liste des documents



Les documents de familles de brevets sont indiqués en annexe

*** Catégories spéciales de documents cités:**

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

29 novembre 2012

Date d'expédition du présent rapport de recherche internationale

12/12/2012

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Savvides, George

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°

PCT/FR2012/052289

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
FR 2935510	AI	05-03-2010	EP 2160002 AI 03-03-2010
			FR 2935510 AI 05-03-2010
			JP 2010061659 A 18-03-2010
			US 2010058463 AI 04-03-2010
