(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
7 avril 2016 (07.04.2016)

WIPO | PCT

(10) Numéro de publication internationale
WO 2016/051059 A1

(51) Classification internationale des brevets :
H04W 12/10 (2009.01) *H04W 88/02* (2009.01)
H04W 12/12 (2009.01)

(21) Numéro de la demande internationale :
PCT/FR2015/052579

(22) Date de dépôt international :
28 septembre 2015 (28.09.2015)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1459326 30 septembre 2014 (30.09.2014) FR

(71) Déposant : **ORANGE** [FR/FR]; 78 rue Olivier de Serres, 75015 Paris (FR).

(72) Inventeurs : **SABT, Mohamed**; 12 rue Saint-Ouen, 14000 Caen (FR). **ACHEMLAL, Mohammed**; 9 rue de la Masse, 14000 Caen (FR).

(74) Mandataire : **ORANGE/IPL**; RENARD Béatrice, 38-40 rue du Général Leclerc, 92794 Issy Moulineaux Cedex 9 (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, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, 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, SA, 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.

(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, ST, 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, KM, ML, MR, NE, SN, TD, TG).

Publiée :

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

(54) **Title** : METHOD OF PROTECTING A MOBILE TERMINAL AGAINST ATTACKS

(54) **Titre** : PROCÉDÉ DE PROTECTION D'UN TERMINAL MOBILE CONTRE DES ATTAQUES

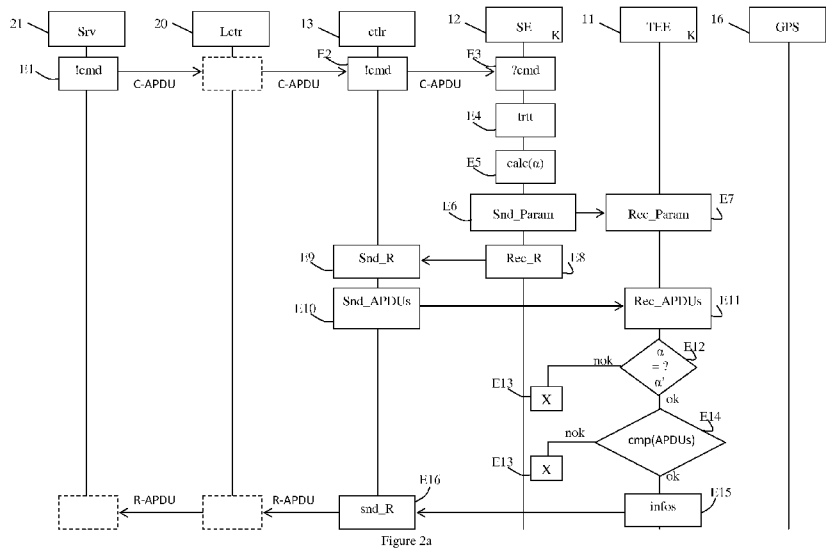

Figure 2a

E15 Info

(57) **Abstract** : The invention relates to a method of detecting an attack aimed at a mobile terminal (10), the terminal comprising a security element (12), a contactless controller (13) suitable for dialoguing with a contactless reader (20) and a secure execution environment (11), in which: - any command (C-APDU) originating from the contactless reader and received by the contactless controller is dispatched to the secure execution environment and to the security module, and - any command (C-APDU) received by the security element is dispatched to the secure execution environment, the method comprising a step of verification (E14), implemented by the secure execution environment, in the course of which it is verified that to a command (C-APDU) received from the contactless controller there corresponds a same command (C-APDU) received from the security element, in the converse case a software attack of relay type is detected.

(57) **Abrégé** :

[Suite sur la page suivante]

WO 2016/051059 A1

L'invention concerne un procédé de détection d'une attaque visant un terminal mobile (10), le terminal comprenant un élément de sécurité (12), un contrôleur sans contact (13) adapté pour dialoguer avec un lecteur sans contact (20) et un environnement d'exécution sécurisée (11), dans lequel : - toute commande (C-APDU) en provenance du lecteur sans contact et reçue par le contrôleur sans contact est envoyée à l'environnement d'exécution sécurisée et au module de sécurité, et - toute commande (C-APDU) reçue par l'élément de sécurité est envoyée à l'environnement d'exécution sécurisée, le procédé comprenant une étape de vérification (E14), mise en œuvre par l'environnement d'exécution sécurisée, au cours de laquelle il est vérifié qu'à une commande (C-APDU) reçue du contrôleur sans contact correspond une même commande (C-APDU) reçue de l'élément de sécurité, dans le cas contraire une attaque logicielle de type relais est détectée.

Procédé de protection d'un terminal mobile contre des attaques

La présente invention concerne un procédé de protection d'un terminal mobile contre des attaques, plus précisément contre des attaques de type relais.

Elle trouve une application particulièrement intéressante dans la sécurisation de services sensibles, tels que des services de paiement sur terminaux mobiles intelligents.

Un terminal mobile intelligent de type smartphone en anglais, adapté pour exécuter des services sans contact sensibles, tels qu'un service de paiement de type « NFC » (de l'anglais « Near Field Communication »), comprend de manière classique un élément de sécurité (ou « SE », de l'anglais « Secure Element »), par exemple une carte « SIM » (de l'anglais « Subscriber Identity Module ») et un contrôleur NFC. Le contrôleur NFC est agencé pour communiquer avec un lecteur NFC relié, dans le cadre d'une transaction de paiement, à un terminal marchand. L'élément de sécurité est adapté pour mémoriser des données et applications sensibles. Dans le cas de transactions de paiement, l'élément de sécurité mémorise des données cryptographiques de types clés secrètes ou clés privées, des applications sensibles ; l'accès à des opérations sensibles de l'application, voire l'accès à l'application de paiement elle-même, est conditionné par la saisie par l'utilisateur d'un code personnel d'identification (on parle habituellement de code « PIN », de l'anglais « Personal Identification Number »). Lorsque l'utilisateur souhaite initier une transaction de paiement chez un marchand, il approche son terminal mobile du lecteur NFC situé chez le marchand et l'application de paiement localisée dans l'élément de sécurité s'exécute entre le terminal et le serveur par l'intermédiaire du lecteur et du contrôleur NFC, les informations relatives à la transaction étant échangées entre l'application de paiement et le lecteur NFC au moyen de trames « APDU » (de l'anglais « Application Protocol Data Unit »). Au terme de la transaction, le compte de l'utilisateur est débité du montant de la transaction.

Une telle architecture est cependant sensible à des attaques de type relais. Pour mettre en place une telle attaque, une personne malveillante installe sur le terminal mobile de l'utilisateur victime de l'attaque un logiciel malveillant destiné à rediriger des données vers le terminal mobile de l'attaquant. Cette installation est réalisée par exemple au moyen d'un cheval de Troie, logiciel apparemment légitime du point de vue du terminal mobile de la victime et qui comprend le logiciel malveillant. Le logiciel malveillant est agencé pour écouter et enregistrer des données échangées avec l'élément de sécurité lors de transactions de paiement légitimes. En particulier, des données sensibles telles que le code d'identification personnel, saisi par l'utilisateur légitime pour valider une transaction de paiement peuvent ainsi être accessibles au logiciel malveillant. Par exemple, le code d'identification personnel peut être demandé à

l'utilisateur lors de l'exécution d'une fonction de sécurité telle qu'une fonction de signature qui nécessite d'accéder à une clé privée de signature mémorisée dans le module de sécurité.

L'attaquant installe également un logiciel de contrôle sur son propre terminal mobile. Le logiciel de contrôle est agencé pour contrôler les actions du logiciel malveillant installé sur le terminal de la victime et pour relayer astucieusement, via le réseau Internet, des informations du terminal de la victime vers le terminal de l'attaquant ou du terminal de l'attaquant vers le terminal de la victime.

Ainsi, dans un premier exemple d'attaque, l'attaquant initie une transaction de paiement chez un marchand. Les échanges entre l'élément de sécurité du terminal de l'attaquant et le terminal de paiement, via le lecteur et le contrôleur NFC, sont relayés par le logiciel de contrôle du terminal de l'attaquant vers le logiciel malveillant installé sur le terminal de la victime. Le logiciel malveillant commande l'exécution de l'application de paiement du terminal mobile de la victime. Lorsque le code d'identification personnel nécessaire pour accéder à une fonction sensible de l'élément de sécurité de la victime est demandé lors de la transaction, le logiciel malveillant le transmet sans que la victime ne soit sollicitée. Les réponses de l'élément de sécurité de la victime sont ainsi relayées par le logiciel malveillant vers le terminal de l'attaquant qui les transmet au terminal de paiement du marchand via le contrôleur NFC. Ni le marchand, ni la victime ne se rendent compte qu'une attaque a lieu. Cependant, c'est le compte de la victime qui est débité à la place de celui de l'attaquant. Une telle attaque par relais permet ainsi à l'attaquant d'acheter des biens en débitant le compte de la victime.

Dans un deuxième exemple d'attaque, l'attaquant vole des données de type points de fidélité destinés à la victime, plus précisément destinés à être mémorisées dans l'élément de sécurité de la victime. Dans ce cas, c'est la victime qui initie une transaction chez un marchand à travers un lecteur sans contact. Des points de fidélité qui sont transmis en fin de transaction par le marchand au terminal de la victime via le lecteur et le contrôleur NFC sont relayés, via le réseau Internet, par le logiciel malveillant installé sur le terminal de la victime vers le terminal mobile de l'attaquant de manière à être enregistrés dans l'élément de sécurité de l'attaquant.

Ces attaques sont possibles du fait de la connectivité Internet des terminaux intelligents.

Un des buts de l'invention est de remédier à des insuffisances/inconvénients de l'état de la technique et/ou d'y apporter des améliorations.

A cette fin, l'invention propose un procédé de détection d'une attaque visant un terminal mobile, le terminal comprenant un élément de sécurité, un contrôleur sans contact adapté pour dialoguer avec un lecteur sans contact et un environnement d'exécution sécurisée, dans lequel :

- toute commande en provenance du lecteur sans contact et reçue par le contrôleur sans contact est envoyée à l'environnement d'exécution sécurisée et au module de sécurité, et

- toute commande reçue par l'élément de sécurité est envoyée à l'environnement d'exécution sécurisée,

le procédé comprenant une étape de vérification, mise en œuvre par l'environnement d'exécution sécurisée, au cours de laquelle il est vérifié qu'à une commande reçue du contrôleur sans contact correspond une même commande reçue de l'élément de sécurité, dans le cas contraire une attaque logicielle de type relais est détectée.

Le procédé décrit permet ainsi de détecter des attaques logicielles de type relais. En effet, il est vérifié qu'à une commande reçue du contrôleur NFC par l'environnement d'exécution sécurisée correspond la réception par l'environnement d'exécution sécurisée de la même commande en provenance de l'élément de sécurité.

Il est habituel qu'un attaquant qui souhaite mettre en œuvre une attaque logicielle de type relais installe sur le terminal mobile d'une victime un logiciel malveillant, et sur son propre terminal mobile un logiciel de contrôle adapté pour contrôler le logiciel malveillant. Dans un premier scénario d'attaque, l'attaquant initie une transaction de paiement avec son propre terminal mobile via son contrôleur NFC. Il relaie les commandes reçues du lecteur NFC via son propre contrôleur au terminal mobile de la victime grâce au logiciel de contrôle et au logiciel malveillant installé sur le terminal de la victime. C'est l'application de paiement du terminal mobile de la victime qui est exécutée qui est ainsi exécutée. Ainsi, l'élément de sécurité transmet la commande relayée par le logiciel de contrôle du terminal mobile de l'attaquant à l'environnement d'exécution sécurisée du terminal de la victime. L'environnement d'exécution sécurisée ne reçoit cependant pas la même commande en provenance contrôleur NFC. En effet, le contrôleur NFC de la victime n'est pas impliqué dans la transaction puisque c'est celui de l'attaquant qui communique avec le lecteur NFC dans le cadre de la transaction en cours. L'attaque est donc détectée par l'environnement d'exécution sécurisée du terminal de la victime.

Dans un deuxième scénario d'attaque, la victime est en train d'exécuter une transaction au cours de laquelle des points de fidélité vont être transmis à l'élément de sécurité via le contrôleur NFC du terminal de la victime. Le logiciel malveillant commandé par le logiciel de contrôle du terminal de l'attaquant relaie les commandes relatives à cette transmission de points de fidélité vers le terminal de l'attaquant. Une commande reçue par le contrôleur NFC du terminal mobile de la victime est donc envoyée à l'environnement d'exécution sécurisée du terminal de la victime. Cependant, cette même commande n'est pas reçue de l'élément de sécurité de la victime puisqu'elle est traitée par l'élément de sécurité de l'attaquant.

Ainsi, dans ces deux scénarios, la non réception par l'environnement d'exécution sécurisée d'une même commande par deux canaux différents, en l'espèce le canal environnement d'exécution sécurisée/élément de sécurité et le canal environnement d'exécution sécurisée/contrôleur NFC, indique qu'une attaque logicielle de type relais est en cours.

Dans un exemple de réalisation, l'élément de sécurité et l'environnement d'exécution sécurisée partagent la connaissance d'une clé secrète, le procédé comprenant en outre les étapes suivantes :

- calcul par l'élément de sécurité d'une première valeur de contrôle, fonction de la commande reçue du contrôleur sans contact et de la clé secrète, et envoi de ladite première valeur de contrôle à l'environnement d'exécution sécurisée,

- vérification par l'environnement d'exécution sécurisée de la cohérence entre la première valeur de contrôle et la commande reçue de l'élément de sécurité, une attaque logicielle de type relais étant détectée en cas d'incohérence.

Dans cet exemple de réalisation, le calcul de la première valeur de contrôle par l'élément de sécurité, fonction de la clé secrète K et de la commande C-APDU reçue du contrôleur sans contact, et l'envoi de cette valeur à l'environnement d'exécution sécurisée, permet de s'assurer que la commande transmise par l'élément de sécurité à l'environnement d'exécution sécurisée est bien celle qui est reçue par cet environnement. En d'autres termes, la valeur de contrôle permet de vérifier l'intégrité du canal de communication qui sépare l'élément de sécurité de l'environnement d'exécution sécurisée qui, par construction, n'est pas sécurisé. On rappelle que ce lien n'est pas sécurisé car le module de sécurité peut dans certains cas être amovible. Ce contrôle supplémentaire procure un niveau de sécurité supplémentaire dans détection. Ainsi, on s'assure que c'est bien l'élément de sécurité qui partage la clé privée avec l'environnement d'exécution sécurisée et qui est donc dans le même terminal mobile qui envoie la commande.

Dans variante de réalisation, lequel l'élément de sécurité et l'environnement d'exécution sécurisée partagent la connaissance d'une clé secrète, le procédé comprenant en outre les étapes suivantes :

- réception par l'environnement d'exécution sécurisée, en provenance de l'élément de sécurité de la réponse,

- réception par l'environnement d'exécution sécurisée, en provenance du contrôleur sans contact de la réponse à la commande reçue de l'élément de sécurité par le contrôleur,

- calcul par l'élément de sécurité d'une première valeur de contrôle, fonction de la réponse reçue du contrôleur sans contact et de la clé secrète et envoi de ladite première valeur de contrôle à l'environnement d'exécution sécurisée,

- vérification par l'environnement d'exécution sécurisée de la cohérence entre la première valeur de contrôle et la réponse reçue de l'élément de sécurité, une attaque logicielle de type relais étant détectée en cas d'incohérence.

Dans cet exemple de réalisation, la première valeur de contrôle est calculée en fonction de la clé privée et de la réponse déterminée par l'élément de sécurité. Cet exemple est une alternative à l'exemple décrit précédemment.

Dans un autre exemple de réalisation, lequel le calcul de la première valeur de contrôle par l'élément de sécurité est également fonction d'une réponse à ladite commande déterminée par l'élément de sécurité et que le procédé comprend les étapes suivantes :

- réception par l'environnement d'exécution sécurisée, en provenance de l'élément de sécurité de la réponse,

- réception par l'environnement d'exécution sécurisée, en provenance du contrôleur sans contact de la réponse à la commande reçue de l'élément de sécurité par le contrôleur,

- vérification de la cohérence entre la première valeur de contrôle et les commande et réponse reçues de l'élément de sécurité,

- si la vérification est positive, comparaison de la réponse reçue de l'élément de sécurité avec la réponse reçus du contrôleur sans contact, une attaque logicielle de type relais étant détectée si la vérification est négative ou si la comparaison est négative.

Dans cet exemple, la première valeur de contrôle est calculée à partir de la commande et de la réponse déterminée par l'élément de sécurité. Le niveau de sécurité est donc plus élevé que lorsque le contrôle porte sur un seul type de trame.

Avantageusement, le procédé comprend, lorsqu'aucune attaque logicielle de type relais n'a été détectée :

- une étape d'obtention par l'environnement d'exécution sécurisée auprès d'un module de localisation du terminal, de coordonnées de localisation géographique du terminal mobile,

- une étape de comparaison desdites coordonnées de localisation géographique du terminal avec des coordonnées de localisation géographique du lecteur, une attaque matérielle de type relais étant détectée lorsque les coordonnées du terminal et du lecteur diffèrent d'une valeur supérieure à une valeur seuil donnée.

Les étapes du procédé décrites ici permettent de détecter des attaques particulières, en l'espèce, des attaques matérielles de type relais. Ce type d'attaque est plus compliqué à mettre en œuvre pour un attaquant car il nécessite d'installer une sonde dans le terminal mobile d'une victime potentielle. Cette sonde est destinée à relayer vers, ou depuis le terminal de l'attaquant des informations qui transitent sur un lien de communication qui relie le contrôleur NFC à l'environnement d'exécution sécurisée. Avec les étapes du procédé décrites ici, on s'assure que

c'est bien l'environnement d'exécution sécurisée qui est dans le terminal mobile qui communique avec le contrôleur NFC.

L'invention concerne également un terminal mobile comprenant un élément de sécurité, un contrôleur sans contact adapté pour dialoguer avec un lecteur sans contact, et un environnement d'exécution sécurisée, et :

- des premiers moyens d'envoi, agencés pour envoyer toute commande en provenance du lecteur sans contact et reçue par le contrôleur sans contact à l'environnement d'exécution sécurisée et au module de sécurité,

- des deuxièmes moyens d'envoi, agencés pour envoyer toute commande reçue par l'élément de sécurité à l'environnement d'exécution sécurisée,

- des premiers moyens de vérification, agencés pour vérifier qu'à une commande reçue du contrôleur sans contact correspond la même commande reçue de l'élément de sécurité, une attaque logicielle de type relais est détectée en cas de vérification négative.

Dans un autre exemple de réalisation du terminal mobile, l'élément de sécurité et l'environnement d'exécution sécurisée partagent la connaissance d'une clé secrète, le terminal comprenant en outre :

- des moyens de calcul et d'envoi, agencés pour que l'élément de sécurité calcule une première valeur de contrôle, fonction de la commande reçue du contrôleur sans contact et de la clé secrète, et pour envoyer ladite première valeur de contrôle à l'environnement d'exécution sécurisée,

- des deuxièmes moyens de vérification, agencés pour que l'environnement d'exécution sécurisée vérifie la cohérence entre la première valeur de contrôle et la commande reçue de l'élément de sécurité, une attaque logicielle de type relais étant détectée en cas d'incohérence.

Dans un autre exemple de réalisation, le terminal mobile comprend en outre :

- un module de géolocalisation, agencé pour fournir à l'environnement d'exécution sécurisée des coordonnées géographiques du terminal mobile,

- des moyens de réception de coordonnées géographiques du lecteur, agencés pour recevoir des coordonnées géographiques du lecteur,

- des moyens de comparaison, agencés pour, lorsqu'aucune attaque par relais n'a été détectée, comparer les coordonnées du terminal mobile avec les coordonnées géographiques du lecteur, une attaque matérielle étant détectée lorsque les coordonnées du terminal et du lecteur diffèrent d'une valeur supérieure à une valeur seuil donnée.

L'invention concerne aussi un programme d'ordinateur sur un support de données et chargeable dans la mémoire d'un terminal mobile, le programme comprenant des instructions de

code pour l'exécution des étapes du procédé de détection d'attaques selon l'invention, lorsque le programme est exécuté sur ledit ordinateur.

L'invention porte également sur un support de données dans lequel est enregistré le programme selon l'invention.

D'autres caractéristiques et avantages de la présente invention seront mieux compris de la description et des dessins annexés parmi lesquels :

- la figure 1 est une représentation schématique d'une architecture adaptée pour mettre en œuvre les étapes d'un procédé de détection d'attaques, selon un premier exemple de réalisation de l'invention ;
- la figure 2a présente les étapes d'un procédé de détection d'attaques logicielle de type relais, selon un premier exemple de réalisation de l'invention ;
- la figure 2b présente les étapes d'un procédé de détection d'attaques matérielle, selon un exemple de réalisation de l'invention ;
- la figure 3 est une représentation schématique fonctionnelle d'un terminal mobile, selon un exemple de réalisation de l'invention.

Une architecture adaptée pour mettre en œuvre les étapes du procédé de détection d'attaques, selon un premier exemple de réalisation de l'invention, va maintenant être décrite en relation avec la figure 1.

Dans cette architecture, un terminal mobile 10 est conforme aux spécifications proposées par l'association GlobalPlatform, ou conforme à des approches similaires. Les spécifications GlobalPlatform définissent une architecture de terminal mobile où coexistent deux environnements d'exécution : un environnement d'exécution sécurisée 11, ou « TEE » (de l'anglais « Trusted Execution Environment ») et un environnement d'exécution non sécurisée, ou « REE » (de l'anglais « Rich Execution Environment ») (non représenté sur la figure 1). L'environnement d'exécution sécurisée 11 est indépendant de l'environnement d'exécution non sécurisée. Il est destiné à offrir un environnement logiciel et matériel pour des applications sécurisées. Il est considéré de confiance et s'appuie sur ses propres ressources : un système d'exploitation sûr, des modules logiciels sûrs et des ressources matérielles sûres, comme des fonctions de sécurité telles qu'un stockage sûr, des interfaces de communication avec des composants de sécurité, etc. L'environnement d'exécution sécurisée 11 est agencé pour fournir des services de sécurité à l'environnement d'exécution non sécurisé au moyen d'interfaces prédéfinies. Il est connu des spécifications GlobalPlatform que le système d'exploitation de l'environnement d'exécution sécurisée 11 est exécuté à partir d'un microprogramme approuvé

(on parle de « firmware » en anglais) qui est authentifié et isolé du système d'exploitation non sécurisé durant le processus de démarrage (on parle de « boot » en anglais). Une fois le microprogramme authentifié, le système d'exploitation sécurisée 11 est exécuté et l'environnement d'exécution sécurisée 11 est établi. Lors de cet établissement, l'environnement d'exécution sécurisée 11 initialise le microprogramme, importe des données cryptographiques telles que des clés, des certificats, des signatures et configure certains périphériques afin de garantir la sécurité lors de communications entre l'environnement d'exécution sécurisée 11 et ces périphériques. Au terme de l'établissement de l'environnement d'exécution sécurisée 11, le contrôle est transmis à l'environnement d'exécution non sécurisée. Le démarrage du terminal se poursuit alors avec une exécution du système d'exploitation non sécurisé et un établissement lors de cette exécution de l'environnement d'exécution non sécurisée. Si ensuite l'utilisateur sélectionne une application sécurisée, le système bascule vers l'environnement d'exécution sécurisée et exécute l'application dans cet environnement sûr. Dès la fin de l'exécution de l'application, le système bascule de nouveau vers l'environnement d'exécution non sécurisée.

Le terminal mobile 10 comprend également un élément de sécurité 12. L'élément de sécurité 12 est par exemple une carte « UICC » (pour « Universal Integrated Circuit Card »), telle une carte d'identité d'abonné ou carte « SIM » (de l'anglais « Subscriber Identity Module »), amovible ou soudée (on parle alors « d'embedded SIM »). Dans un autre exemple de réalisation, l'élément de sécurité est un composant amovible de type microSD (« SD » pour Sandisk ®). Dans un autre exemple de réalisation, l'élément de sécurité est une zone logicielle sécurisée. L'élément de sécurité 12 est agencé pour mémoriser des applications ou fonctions sensibles, par exemple une application de paiement, des fonctions et des données cryptographiques telles que des fonctions de signature, des clés secrètes, etc. L'application de paiement comprend des instructions de code pour mettre en œuvre certaines des étapes du procédé de détection d'attaque. Dans un exemple de réalisation, l'application de paiement est mémorisée dans l'environnement d'exécution sécurisée 11 et fait appel à une ou plusieurs fonctions sensibles mémorisées dans l'élément de sécurité 12, par exemple une fonction de signature qui nécessite, pour débloquer l'accès à une clé privée de signature, la saisie par l'utilisateur d'un code PIN correct. Dans un autre exemple de réalisation, l'application de paiement est mémorisée dans l'élément de sécurité 12. Le terminal mobile 10 comprend également un contrôleur sans contact, par exemple un contrôleur « NFC » 13 (de l'anglais « Near Field Communication ») agencé pour permettre une communication sans contact avec un lecteur sans contact, par exemple un lecteur NFC 20 relié à un serveur 21 distant, par exemple le serveur d'un marchand. Lorsque l'application de paiement est exécutée, elle dialogue avec une application du marchand qui s'exécute dans le serveur 21 via le contrôleur NFC 13 et le lecteur

NFC 20. Le contrôleur NFC 13 comprend des instructions de code pour mettre en œuvre celles des étapes du procédé de détection d'attaques qui sont exécutées par le contrôleur NFC 13. Dans un exemple de réalisation, le terminal mobile 10 comprend également un module de géolocalisation, par exemple un module « GPS » 16 (de l'anglais « Global Positioning System ») destiné à fournir des coordonnées de localisation du terminal mobile. Les coordonnées géographiques fournies par le module de géolocalisation 16 sont exprimées par exemple par un couple (X, Y) où X représente la latitude en degrés, minutes, secondes et millièmes de secondes et Y la longitude en degrés, minutes, secondes et millièmes de seconde. Dans un exemple de réalisation, la technique de localisation géographique utilisée par le module 16 est différentielle ; cette technique est plus précise qu'une localisation GPS standard.

On suppose que lors du démarrage de l'environnement d'exécution sécurisée 11, celui-ci a configuré le contrôleur NFC 13 et le module GPS 16 le cas échéant, de manière à garantir la sécurité des communications qu'il établit avec ces périphériques. Ainsi, d'un point de vue logiciel les échanges entre l'environnement d'exécution sécurisée 11 et le contrôleur NFC 13 d'une part, et entre l'environnement d'exécution sécurisée 11 et le module GPS 16 d'autre part sont supposés sécurisés.

On suppose par ailleurs que dans un exemple de réalisation, l'élément de sécurité 12 et l'environnement d'exécution sécurisée 11 partagent la connaissance d'une clé secrète K destinée à garantir que des commandes reçues du lecteur NFC 13 et des réponses qui sont transmises en réponse au lecteur 20 proviennent bien du module de sécurité du terminal mobile qui est en train de réaliser la transaction.

Lors de l'exécution de l'application de paiement qui réside dans l'environnement d'exécution sécurisée 11 ou dans l'élément de sécurité 12, des informations relatives à la transaction sont transportées au format APDU (de l'anglais « Application Protocol Data Unit ») entre le lecteur NFC 20, l'environnement d'exécution sécurisée 11 et l'élément de sécurité 12, par l'intermédiaire du contrôleur NFC 13.

Les étapes d'un procédé de détection d'attaques sur un terminal mobile, selon un premier exemple de réalisation de l'invention, vont maintenant être décrites en relation avec la figure 2a.

Un utilisateur, équipé d'un terminal mobile 10 conforme à la description présentée dans l'architecture décrite en relation avec la figure 1 souhaite exécuter une application sans contact, telle une application de paiement NFC mémorisée dans l'élément de sécurité 12 de son terminal mobile10.

Dans une phase préalable de configuration, il a été installé dans l'élément de sécurité 12 et dans l'environnement d'exécution sécurisée 11 du terminal mobile 10 une clé secrète K, partagée par ces deux entités. Dans un exemple de réalisation, l'installation a été faite en usine, avant que le terminal mobile 10 ne soit commercialisé. Dans un autre exemple de réalisation, la clé secrète K a été installée après la mise sur le marché du terminal 10. Par exemple, elle a été installée dans l'élément de sécurité 12 au moyen d'une procédure « OTA » (de l'anglais « Over The Air ») et dans l'environnement d'exécution sécurisée 11 au moyen d'une procédure similaire, via le réseau Internet 3G ou 4G.

Dans une étape initiale (non représentée), l'utilisateur, équipé de son terminal mobile 10 s'approche du lecteur NFC 20 afin de réaliser une transaction sans contact. Dans un exemple de réalisation, le lecteur NFC 20, situé dans une gare, permet à l'utilisateur d'acheter des billets de train au moyen de son terminal mobile 10. Approcher le terminal mobile 10 du lecteur NFC 20 déclenche l'exécution d'une application de paiement mémorisée dans l'élément de sécurité 12 du terminal mobile 10. Dans un autre exemple de réalisation, l'utilisateur du terminal mobile 10 déclenche l'exécution de l'application de paiement en sélectionnant celle-ci dans un menu, puis approche son terminal mobile 10 du lecteur NFC 20. Il s'établit alors un dialogue entre l'application de paiement mémorisée dans l'élément de sécurité 12 et un module de paiement (non représenté sur la figure 2) du marchand mémorisé dans le serveur distant 21, via le lecteur NFC 20 et le contrôleur NFC 13 du terminal 10. Les informations échangées lors de ce dialogue, sous forme de commandes et de réponses, sont transportées dans des trames « APDU » (de l'anglais « Application Protocol Data Unit »).

Dans une étape E1 d'envoi de commande, une commande C-APDU est envoyée du serveur 21 à l'élément de sécurité 12, plus précisément à l'application de paiement située dans l'élément de sécurité 12, via le lecteur NFC 20 et le contrôleur NFC 13. La commande C-APDU est reçue par le contrôleur NFC 13 dans une étape E2 de réception et de retransmission, puis transmise à l'élément de sécurité 12. La commande C-APDU est reçue par l'élément de sécurité 12, plus précisément par l'application de paiement mémorisée dans l'élément de sécurité 12, dans une étape E3 de réception. La commande C-APDU est par exemple une demande de données : demande de confirmation du montant du billet, demande de confirmation du trajet, demande de validation de paiement, etc.

Cette commande C-APDU est traitée par l'élément de sécurité 12 dans une étape E4 de traitement. L'élément de sécurité 12 détermine une réponse R-APDU suite à ce traitement. Par exemple, si la commande C-APDU reçue est une demande de confirmation de trajet, un message est affiché à l'attention de l'utilisateur qui confirme ou non le trajet. La réponse R-APDU comprend alors la réponse de l'utilisateur. Si la commande C-APDU est un message de

validation du paiement, il est demandé à l'utilisateur de saisir un code PIN de service. La saisie d'un code PIN correct déclenche l'exécution d'une fonction de sécurité, par exemple une signature des informations de paiement relatives à la transaction en cours, au moyen d'une clé privée de signature mémorisée dans l'élément de sécurité 12. Dans ce cas, la réponse R-APDU déterminée par l'élément de sécurité 12 est un message qui comprend la signature des informations de paiement.

Dans une étape E5 de calcul d'une première valeur de contrôle, l'élément de sécurité 12, plus précisément l'application de paiement, calcule une première valeur de contrôle α. La première valeur de contrôle α est calculée en appliquant une fonction cryptographique f à la commande C-APDU reçue du contrôleur NFC 13 au cours de l'étape E3 de réception, et à la réponse R-APDU déterminée par l'élément de sécurité 12. La fonction cryptographique f est paramétrée par la clé secrète K partagée par l'élément de sécurité 12 et l'environnement d'exécution sécurisée 11. La fonction cryptographique f est par exemple une fonction d'authentification de type « MAC » (de l'anglais « Message Authentication Code »), par exemple la fonction « HMAC » (pour « Keyed-Hashed MAC »), ou la fonction « CMAC » (pour « Cipher-based MAC »). La première valeur de contrôle α est destinée à permettre à l'environnement d'exécution sécurisée 11 de vérifier l'intégrité de la commande C-APDU et de la réponse R-APDU qui ont été traitées par l'élément de sécurité 12. Ce contrôle se justifie par le fait que le lien de communication entre l'environnement d'exécution sécurisée 11 et l'élément de sécurité 12 n'est, par construction, pas sécurisé. Un tel contrôle est donc destiné à s'assurer de l'intégrité du canal de communication entre l'élément de sécurité 12 et l'environnement d'exécution sécurisée 11.

Dans une étape E6 d'envoi de paramètres, l'élément de sécurité 12 envoie à l'environnement d'exécution sécurisée 11 un ensemble de paramètres qui comprend la première valeur de contrôle α, la commande C-APDU reçue par l'élément de sécurité 12 au cours de l'étape E3 et la réponse R-APDU qu'il a déterminée au cours de l'étape E4 de traitement. Cet ensemble de paramètres est reçu par l'environnement d'exécution sécurisée 11 dans une étape E7 de réception.

Dans une étape E8 d'envoi, la réponse R-APDU déterminée est envoyée par l'élément de sécurité 12 au contrôleur NFC 13. Elle est reçue par le contrôleur NFC 13 dans une étape E9 de réception.

Dans une étape E10 d'envoi d'informations de transaction, le contrôleur NFC 13 envoie à l'environnement d'exécution sécurisée 11 des informations relatives à la transaction en cours. Dans cet exemple, le contrôleur NFC 13 envoie la commande C-APDU qu'il a reçue du lecteur NFC 20 au cours de l'étape E2 de réception et la réponse R-APDU à cette commande qu'il a

reçue de l'élément de sécurité 12 au cours de l'étape E9 de réception. La commande C-APDU et la réponse R-APDU sont reçues par l'environnement d'exécution sécurisée 11 dans une étape E11 de réception.

Dans une étape E12 de contrôle d'intégrité, l'environnement d'exécution sécurisée 11 vérifie l'intégrité de la commande C-APDU et de la réponse R-APDU reçues de l'élément de sécurité 12 au cours de l'étape E7 de réception. A cette fin il calcule une deuxième valeur de contrôle α' en appliquant la même fonction cryptographique f que celle appliquée par l'élément de sécurité 12 au cours de l'étape E5 de calcul de la première valeur de contrôle α à la commande C-APDU et à la réponse R-APDU reçues du module de sécurité 12 au cours de l'étape E7. La fonction cryptographique f est paramétrée avec la même clé secrète K. Si les deux valeurs de contrôle sont différentes, c'est-à-dire si $\alpha \neq \alpha'$ (branche « nok » sur la figure 2), cela signifie que les données envoyées par le module de sécurité 12 diffèrent de celles reçues par l'environnement d'exécution sécurisée 11. Ce peut être le cas lorsque la première valeur de contrôle α a été calculée au moyen d'une clé secrète différente de celle utilisée par l'environnement d'exécution sécurisée 11 pour calculer la deuxième valeur de contrôle α', ou lorsque les commande C-APDU et réponse R-APDU reçues de l'élément de sécurité 12 diffèrent de celles utilisées par l'élément de sécurité 12 pour calculer la première valeur de contrôle α. Cela peut signifier que ce n'est pas le module de sécurité 12 présent dans le terminal mobile 10 qui a calculé la première valeur de contrôle α. Dans ce cas le procédé se termine dans une étape E13 de fin, ce qui met fin à la transaction en cours. Dans une étape optionnelle suivante (non représentée sur la figure 2), un message d'information est affiché à l'attention de l'utilisateur et/ou envoyé par l'environnement d'exécution sécurisée 11 au lecteur NFC 20.

Dans un deuxième cas où les deux valeurs de contrôle sont identiques, c'est-à-dire où $\alpha = \alpha'$ (branche « ok » sur la figure 2), cela signifie que la commande C-APDU et la réponse R-APDU envoyées par l'élément de sécurité 12 sont bien celles qui ont été reçues par l'environnement d'exécution sécurisée 11. Dans ce cas, dans une étape E14 de vérification, l'environnement d'exécution sécurisée 11 vérifie que les commandes C-APDUs et les réponses R-APDUs reçues d'une part de l'élément de sécurité 12 au cours de l'étape E7 et d'autre part du contrôleur NFC 13 au cours de l'étape E11 sont identiques. Dans un premier cas où elles sont différentes (branche « nok » sur la figure 2), cela signifie que la commande C-APDU et/ou la réponse R-APDU reçues du contrôleur NFC 13 sont différentes de la commande C-APDU et/ou de la réponse R-APDU reçue et traitée par l'élément de sécurité 12. Dans ce cas, une attaque par relais est en cours. Le procédé se termine dans l'étape E13 de fin, ce qui met fin à la transaction en cours. Dans une étape optionnelle suivante (non représentée sur la figure 2), un message d'information est affiché à l'attention de l'utilisateur et/ou envoyé par l'environnement

d'exécution sécurisée 11 au lecteur NFC 14. Dans un deuxième cas où les commandes C-APDUs et les réponses R-APDUs reçues respectivement du contrôleur NFC 13 et de l'élément de sécurité 12 sont identiques (branche « ok » sur la figure), on considère qu'il n'y a pas d'attaque logicielle par relais en cours sur le terminal mobile 10. La transaction peut continuer. L'environnement d'exécution sécurisée 11 en informe le contrôleur NFC 13 dans une étape E15 d'informations. Le contrôleur NFC 13 peut envoyer la réponse R-APDU au serveur 21 via le lecteur NFC 20 dans une étape E16 de réponse et une nouvelle commande (non représentée) peut être reçue du serveur 15 via le lecteur 14 et le contrôleur 13 et traitée comme décrit précédemment.

Les étapes décrites précédemment permettent de détecter qu'aucune attaque logicielle de type relais n'est en cours. Il existe cependant un risque qu'une attaque plus difficile à mettre en œuvre soit en cours. Cette attaque est qualifiée d'attaque matérielle puisqu'elle nécessite d'installer une sonde sur un bus de communication qui relie l'environnement d'exécution sécurisée 11 à l'élément de sécurité 12. Les étapes décrites en relation avec la figure 2b, optionnelles, sont mises en œuvre pour détecter une attaque matérielle de type relais lorsqu'aucune attaque logicielle de type relais n'a été détectée. Elles sont mises en œuvre après l'étape E14 de comparaison et dans le cas où la comparaison est positive (branche « ok » sur la figure 2).

Lorsque l'on souhaite détecter une telle attaque matérielle, dans une étape E17 de requête de coordonnées, mise en œuvre lorsque les première et deuxième valeurs de contrôle α et α' sont identiques, l'environnement d'exécution sécurisée 11 demande au module de localisation GPS 16 les coordonnées géographiques (X, Y) du terminal mobile 10. Cette requête est reçue par le module de localisation GPS 16 dans une étape E18 de réception. Le module de localisation GPS 16 envoie les coordonnées géographiques du terminal mobile 10 dans une étape E19 d'envoi des coordonnées géographiques. Les coordonnées géographiques sont reçues par l'environnement d'exécution sécurisée 11 dans une étape E20 de réception.

Dans une étape E21 de comparaison, l'environnement d'exécution sécurisée 12 compare les coordonnées géographiques (X, Y) du terminal mobile 10 avec les coordonnées géographiques (X', Y') du lecteur NFC 20. Dans un exemple de réalisation, les coordonnées géographiques (X', Y') du lecteur NFC 20 sont fournies par le lecteur 20 au contrôleur NFC 13 au début de l'exécution de l'application de paiement. Elles sont transmises du contrôleur NFC 13 à l'environnement d'exécution sécurisée 11 spontanément, ou sur requête de l'environnement d'exécution sécurisée 11 dans une étape préalable non représentée sur la figure 2.

La comparaison entre les coordonnées (X, Y) du terminal mobile et les coordonnées (X', Y') du lecteur NFC 20 est positive si la différence entre les deux ensembles de coordonnées (X, X') et (Y, Y') est inférieure à un seuil prédéfini. Au-dessous de ce seuil, il est considéré que les données de localisation géographiques associées au terminal mobile 10 et les coordonnées géographiques (X', Y') du lecteur NFC 20 sont suffisamment proches l'une de l'autre pour que l'on considère que le terminal mobile 10 et le lecteur NFC 14 sont les deux équipements qui sont effectivement impliqués dans la transaction en cours. Dans un système de localisation où les coordonnées comprennent une latitude et une longitude exprimées en degrés, minutes, secondes et millièmes de seconde, un seuil prédéfini peut consister à n'autoriser des variations que de l'ordre d'une dizaine de millièmes de secondes pour la latitude et la longitude, ce qui représente une trentaine de centimètres.

Dans un premier cas où la différence entre les deux ensembles de coordonnées est inférieure au seuil prédéfini (branche « ok » sur la figure 2), alors il est confirmé qu'aucune attaque par relais n'est en cours. L'environnement d'exécution sécurisée 11 en informe le contrôleur NFC 13 dans l'étape E15 d'informations. Le contrôleur NFC 13 peut envoyer la réponse R-APDU au serveur 21 via le lecteur NFC 20 dans une étape E16 de réponse et une nouvelle commande (non représentée) peut être reçue du serveur 15 via le lecteur 14 et le contrôleur 13 et traitée comme décrit précédemment.

Dans un deuxième cas où la différence est supérieure au seuil prédéfini, (branche « nok » sur la figure 2) alors on considère qu'une attaque matérielle de type relais est en cours puisque le terminal 10 et le lecteur NFC 14 sont trop éloignés l'un de l'autre pour exécuter la transaction de paiement en cours. Dans ce cas le procédé s'arrête dans l'étape E13 de fin, ce qui met fin à la transaction en cours. Dans une étape optionnelle suivante (non représentée), un message d'information est affiché à l'attention de l'utilisateur et/ou envoyé par l'environnement d'exécution sécurisée 11 au lecteur NFC 20.

L'attaque matérielle de type relais est cependant compliquée à mettre en œuvre. Les étapes optionnelles E17 à E21 permettent ainsi de s'assurer que c'est bien l'environnement d'exécution sécurisée 11 du terminal mobile 10 qui effectue la comparaison entre les première et deuxième valeurs de contrôle et qui fournit le résultat de cette comparaison au contrôleur NFC.

Dans un deuxième exemple de réalisation (non représenté sur la figure 2), le contrôle effectué par l'environnement d'exécution sécurisée 11 au cours des étapes E12 et E14 porte uniquement sur la commande C-APDU. Ainsi, la première valeur de contrôle α est calculée par l'élément de sécurité 12 au cours de l'étape E5 en appliquant la fonction cryptographique f à la

clé secrète K et à la commande C-APDU reçue du contrôleur NFC 13. Dans cet exemple, seules la première valeur de contrôle α et la commande C-APDU sont envoyées à l'environnement d'exécution sécurisée 11 au cours de l'étape E6 d'envoi de paramètres de contrôle. Dans l'étape E12 de vérification, la deuxième valeur de contrôle α' est calculée par l'environnement d'exécution sécurisée 11 en appliquant la fonction cryptographique f à la clé secrète K et à la commande C-APDU reçue du contrôleur NFC. Si les valeurs sont égales, alors dans l'étape E14, seules les commandes C-APDUs reçues par l'environnement d'exécution sécurisée 11 d'une part du contrôleur NFC 13 au cours de l'étape E11 et d'autre part de l'élément de sécurité 12 au cours de l'étape E7 sont comparées. Le procédé est ici plus léger à mettre en œuvre en ce sens que seules les commandes C-APDU sont comparées. Dans une variante de réalisation, le contrôle est similaire à celui décrit dans cet exemple hormis qu'il concerne la réponse R-APDU au lieu de la commande C-APDU.

Dans un troisième exemple de réalisation (non représenté sur la figure 3), un contrôle minimal est mis en œuvre par l'environnement d'exécution sécurisée 11 afin de détecter une attaque par relais. Ce contrôle consiste à s'assurer qu'à toute commande C-APDU reçue du contrôleur de sécurité 13 par l'environnement d'exécution sécurisée 11 correspond une même commande C-APDU reçue de l'élément de sécurité 12 par l'environnement d'exécution sécurisée 11. Dans cet exemple de réalisation, l'étape E5 de calcul de la première valeur de contrôle α n'est pas exécutée et l'étape E6 d'envoi de paramètres consiste à envoyer la commande C-APDU de l'élément de sécurité 12 à l'environnement d'exécution sécurisée 11. Dans cet exemple, le contrôleur NFC 13 envoie à l'environnement d'exécution sécurisée 11 au cours de l'étape E10 la commande C-APDU. Dans une variante de réalisation, la commande C-APDU peut être envoyée par le contrôleur NFC 13 à l'environnement d'exécution sécurisée 11 au cours de l'étape E3, en même temps qu'il l'envoie à élément de sécurité 12. Dans l'exemple décrit ici, l'étape E12 n'est pas exécutée et l'étape E14 consiste pour l'environnement d'exécution sécurisée 11 à comparer les commandes C-APDU reçues respectivement de l'élément de sécurité 12 et du contrôleur NFC 13.

Une description fonctionnelle d'un terminal mobile 10 selon un premier exemple de réalisation de l'invention, va maintenant être fournie en relation avec la figure 3.

Le terminal mobile 10 est un terminal intelligent de type smartphone en anglais. Il est conforme aux spécifications GlobalPlatform. Il comprend ainsi un environnement d'exécution sécurisée 101, ou TEE, et un environnement d'exécution non sécurisée (non représenté sur la figure 3). Il comprend également :

- un élément de sécurité 12, adapté pour héberger des applications et/ou des fonctions sensibles. Dans un exemple de réalisation, il héberge une application de paiement sans contact ;
- un contrôleur NFC 11 adapté pour dialoguer avec le lecteur sans contact NFC 20 (non représenté sur la figure 3), l'élément de sécurité 12 et l'environnement d'exécution sécurisée 11, et pour échanger des informations sous forme de trames APDU ;
- le cas échéant, un module de géolocalisation 16, adapté pour fournir les coordonnées géographiques du terminal mobile 10.

L'environnement d'exécution sécurisée 11 est un environnement qui fonctionne en parallèle de l'environnement d'exécution non sécurisée. Les applications sensibles en termes de sécurité sont alors exécutées soit dans l'élément de sécurité, soit dans l'environnement d'exécution sécurisée. L'environnement d'exécution sécurisée fournit des fonctions de sécurité telles qu'un espace de stockage sécurisé, un espace d'exécution d'applications sécurisé et une gestion sécurisée d'interfaces d'entrée/sortie. Certains canaux de communication sont alors nativement sécurisée par l'environnement d'exécution sécurisée 11, comme le lien TEE/contrôleur NFC 13, ou le lien TEE/écran tactile (l'écran tactile n'est pas représenté sur la figure 3). Par contre, le lien TEE/élément de sécurité n'est, par construction pas sécurisé.

Le terminal mobile 10 comprend également un ensemble de ressources décrites ici de manière simplifiée comme étant réparties entre les différents éléments du terminal mobile 10. Cette description simplifiée est cohérente avec la description du procédé dans laquelle on considère que les étapes sont mises en œuvre dans le terminal mobile. Ainsi, de manière schématique, le terminal mobile 10 comprend :

- une unité de traitement 101, ou « CPU » pour « Central Processing Unit », 101-1,
- un ensemble de mémoires, dont une mémoire volatile 102 et une mémoire de stockage 103. La mémoire volatile 102 est agencée pour exécuter des instructions de code, stocker des variables, etc. La mémoire de stockage 103 est agencée pour mémoriser des données de sécurité telles que des clés, des signatures, etc., le cas échéant la clé secrète K, ainsi qu'un programme sécurisé comprenant des instructions de code destinées à mettre en œuvre les étapes du procédé de détection d 'attaques telles que décrites précédemment. On comprend que par exemple, la clé secrète K, partagée entre l'élément de sécurité 12 et l'environnement d'exécution sécurisée 11 est mémorisée dans une première zone mémoire sécurisée, propre à l'élément de sécurité 12 et une deuxième zone mémoire sécurisée, propre à l'environnement d'exécution sécurisée 11.

Le terminal mobile 10 comprend également :

- des premiers moyens d'envoi 104, agencés pour envoyer toute commande C-APDU en provenance du lecteur NFC 20 et reçue par le contrôleur NFC 13 à l'environnement d'exécution sécurisée 11 et à l'élément de sécurité 12 ;
- des deuxièmes moyens d'envoi 105, agencés pour envoyer toute commande C-APDU reçue par l'élément de sécurité 12 à l'environnement d'exécution sécurisée 11 ;
- des premiers moyens de vérification 106, agencés poru vérifier qu'à une commande C-APDU reçue du contrôleur NFC 13 correspond une même commande C-APDU reçue de l'élément de sécurité 12, une attaque logicielle de type relais étant détectée en cas de vérification négative.

Dans un exemple de réalisation, le terminal mobile 10 comprend également les modules suivants, en pointillés sur la figure 3 :

- des moyens 107 de calcul et d'envoi, agencés pour que l'élément de sécurité 12 calcule une première valeur de contrôle, fonction de la commande C-APDU reçue du contrôleur NFC 13 et de la clé secrète K partagée entre l'environnement d'exécution sécurisée et l'élément de sécurité 12, et pour envoyer la valeur de contrôle ainsi calculée à l'environnement d'exécution sécurisée,
- des deuxièmes moyens de vérification 108, agencés pour que l'environnement d'exécution sécurisée 11 vérifie la cohérence entre la première valeur de contrôle et la commande reçue de l'élément de sécurité 12, une attaque logicielle de type relais étant détectée en cas d'incohérence.

Dans un exemple de réalisation, le terminal mobile 10 comprend également :

- des moyens 109 de réception de coordonnées géographiques, agencés pour recevoir du lecteur 14 ses coordonnées géographiques,
- des moyens de comparaison 110, agencés pour comparer, lorsqu'aucune attaque logicielle de type relais n'a été détectée, les coordonnées du terminal mobile 10 avec les coordonnées géographiques du lecteur 20, une attaque matérielle étant détectée lorsque les coordonnées du terminal mobile 10 et du lecteur 20 diffèrent d'une valeur supérieure à une valeur seuil donnée.

Les premiers moyens d'envoi 104, les deuxièmes moyens d'envoi 105, les premiers moyens de vérification 106, les moyens 107 de calcul et d'envoi, les deuxièmes moyens de vérification 108, les moyens 109 de réception de coordonnées géographiques et les moyens de comparaison 110 sont de préférence des modules logiciels qui comprennent des instructions de code pour faire exécuter les étapes du procédé de détection d'attaques tel que décrit

précédemment. Les modules logiciels peuvent être stockés dans, ou transmis par un support de données. Celui-ci peut être un support matériel de stockage, par exemple un CD-ROM, une disquette magnétique ou un disque dur, ou bien un support de transmission, ou un réseau.

5

REVENDICATIONS

1. Procédé de détection d'une attaque visant un terminal mobile (10), le terminal comprenant un élément de sécurité (12), un contrôleur sans contact (13) adapté pour dialoguer avec un lecteur sans contact (20) et un environnement d'exécution sécurisée (11), dans lequel :

- toute commande (C-APDU) en provenance du lecteur sans contact et reçue par le contrôleur sans contact est envoyée à l'environnement d'exécution sécurisée et au module de sécurité, et

- toute commande (C-APDU) reçue par l'élément de sécurité est envoyée à l'environnement d'exécution sécurisée,

le procédé comprenant une étape de vérification (E14), mise en œuvre par l'environnement d'exécution sécurisée, au cours de laquelle il est vérifié qu'à une commande (C-APDU) reçue du contrôleur sans contact correspond une même commande (C-APDU) reçue de l'élément de sécurité, dans le cas contraire une attaque logicielle de type relais est détectée.

2. Procédé selon la revendication 1, dans lequel l'élément de sécurité (12) et l'environnement d'exécution sécurisée (11) partagent la connaissance d'une clé secrète (K), le procédé comprenant en outre les étapes suivantes :

- calcul (E5) par l'élément de sécurité d'une première valeur de contrôle (α), fonction de la commande reçue du contrôleur sans contact et de la clé secrète, et envoi de ladite première valeur de contrôle à l'environnement d'exécution sécurisée (11),

- vérification (E12) par l'environnement d'exécution sécurisée de la cohérence entre la première valeur de contrôle et la commande reçue de l'élément de sécurité, une attaque logicielle de type relais étant détectée en cas d'incohérence.

3. Procédé selon la revendication 1, dans lequel l'élément de sécurité (12) et l'environnement d'exécution sécurisée (11) partagent la connaissance d'une clé secrète (K), le procédé comprenant en outre les étapes suivantes :

- réception (E7) par l'environnement d'exécution sécurisée, en provenance de l'élément de sécurité de la réponse (R-APDU),

- réception (E11) par l'environnement d'exécution sécurisée, en provenance du contrôleur sans contact de la réponse à la commande reçue de l'élément de sécurité par le contrôleur,

- calcul (E5) par l'élément de sécurité d'une première valeur de contrôle (α), fonction de la réponse reçue du contrôleur sans contact et de la clé secrète et envoi de ladite première valeur de contrôle à l'environnement d'exécution sécurisée (11),

- vérification (E12) par l'environnement d'exécution sécurisée de la cohérence entre la première valeur de contrôle et la réponse reçue de l'élément de sécurité, une attaque logicielle de type relais étant détectée en cas d'incohérence.

4. Procédé selon la revendication 1 ou la revendication 2, dans lequel le calcul de la première valeur de contrôle par l'élément de sécurité est également fonction d'une réponse (R-APDU) à ladite commande déterminée par l'élément de sécurité et que le procédé comprend les étapes suivantes :

- réception (E7) par l'environnement d'exécution sécurisée, en provenance de l'élément de sécurité de la réponse (R-APDU),

- réception (E11) par l'environnement d'exécution sécurisée, en provenance du contrôleur sans contact de la réponse à la commande reçue de l'élément de sécurité par le contrôleur,

- vérification (E12) de la cohérence entre la première valeur de contrôle et les commande et réponse reçues de l'élément de sécurité,

- si la vérification est positive, comparaison (E14) de la réponse reçue de l'élément de sécurité avec la réponse reçus du contrôleur sans contact, une attaque logicielle de type relais étant détectée si la vérification est négative ou si la comparaison est négative.

5. Procédé selon l'une des revendications précédentes, comprenant, lorsqu'aucune attaque logicielle de type relais n'a été détectée :

- une étape d'obtention (E20) par l'environnement d'exécution sécurisée auprès d'un module (16) de localisation du terminal, de coordonnées de localisation géographique du terminal mobile,

- une étape de comparaison (E21) desdites coordonnées de localisation géographique du terminal avec des coordonnées de localisation géographique du lecteur, une attaque matérielle de type relais étant détectée lorsque les coordonnées du terminal et du lecteur diffèrent d'une valeur supérieure à une valeur seuil donnée.

6. Terminal mobile (10) comprenant un élément de sécurité (12), un contrôleur sans contact (13) adapté pour dialoguer avec un lecteur sans contact, et un environnement d'exécution sécurisée (11), et :

- des premiers moyens d'envoi (104), agencés pour envoyer toute commande (C-APDU) en provenance du lecteur sans contact et reçue par le contrôleur sans contact à l'environnement d'exécution sécurisée et au module de sécurité,

- des deuxièmes moyens d'envoi (105), agencés pour envoyer toute commande (C-APDU) reçue par l'élément de sécurité à l'environnement d'exécution sécurisée,

- des premiers moyens de vérification (106), agencés pour vérifier qu'à une commande reçue du contrôleur sans contact correspond la même commande reçue de l'élément de sécurité, une attaque logicielle de type relais est détectée en cas de vérification négative.

7. Terminal mobile selon la revendication 6, dans lequel l'élément de sécurité (12) et l'environnement d'exécution sécurisée (11) partagent la connaissance d'une clé secrète (K), le terminal comprenant en outre :

- des moyens (107) de calcul et d'envoi, agencés pour que l'élément de sécurité calcule une première valeur de contrôle (α), fonction de la commande reçue du contrôleur sans contact et de la clé secrète, et pour envoyer ladite première valeur de contrôle à l'environnement d'exécution sécurisée (11),

- des deuxièmes moyens de vérification (108), agencés pour que l'environnement d'exécution sécurisée vérifie la cohérence entre la première valeur de contrôle et la commande reçue de l'élément de sécurité, une attaque logicielle de type relais étant détectée en cas d'incohérence.

8. Terminal mobile selon la revendication 6 ou la revendication 7, comprenant en outre :

- un module de géolocalisation (16), agencé pour fournir à l'environnement d'exécution sécurisée des coordonnées géographiques du terminal mobile,

- des moyens (109) de réception de coordonnées géographiques du lecteur, agencés pour recevoir des coordonnées géographiques du lecteur,

- des moyens de comparaison (110), agencés pour, lorsqu'aucune attaque par relais n'a été détectée, comparer les coordonnées du terminal mobile avec les coordonnées géographiques du lecteur, une attaque matérielle étant détectée lorsque les coordonnées du terminal et du lecteur diffèrent d'une valeur supérieure à une valeur seuil donnée.

9. Programme d'ordinateur sur un support de données et chargeable dans la mémoire d'un terminal mobile, le programme comprenant des instructions de code pour l'exécution des étapes du procédé de détection d'attaques selon l'une des revendications 1 à 5, lorsque le programme est exécuté sur ledit ordinateur.

10. Support de données dans lequel est enregistré le programme selon la revendication 9.

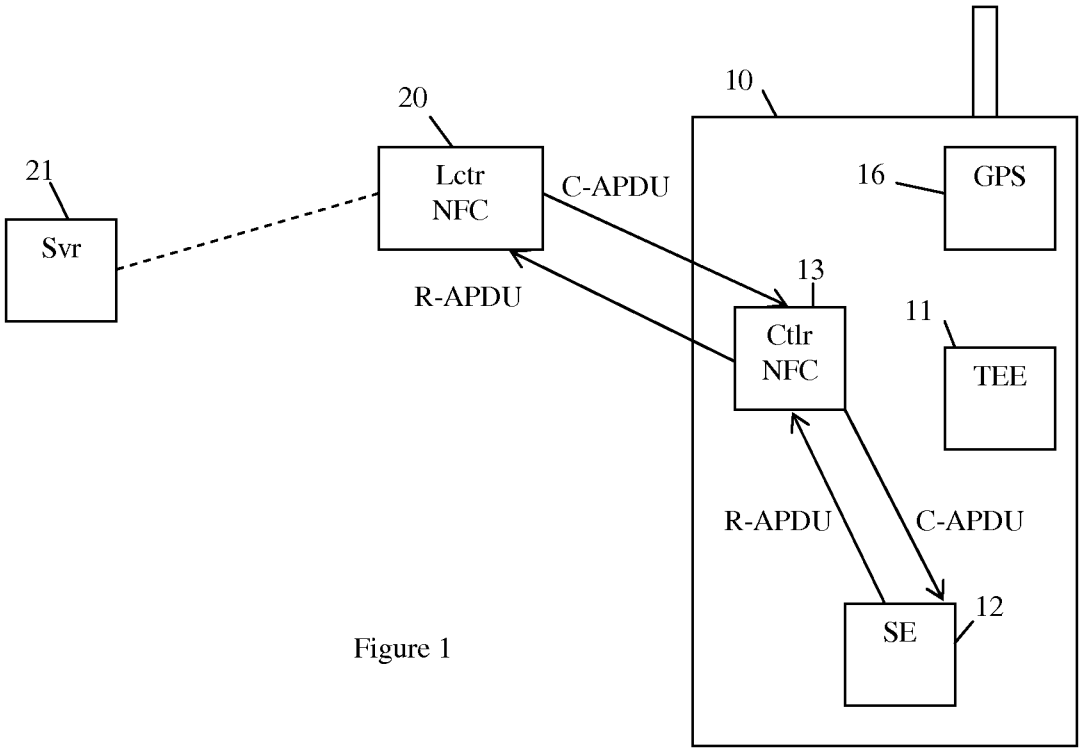

Figure 1

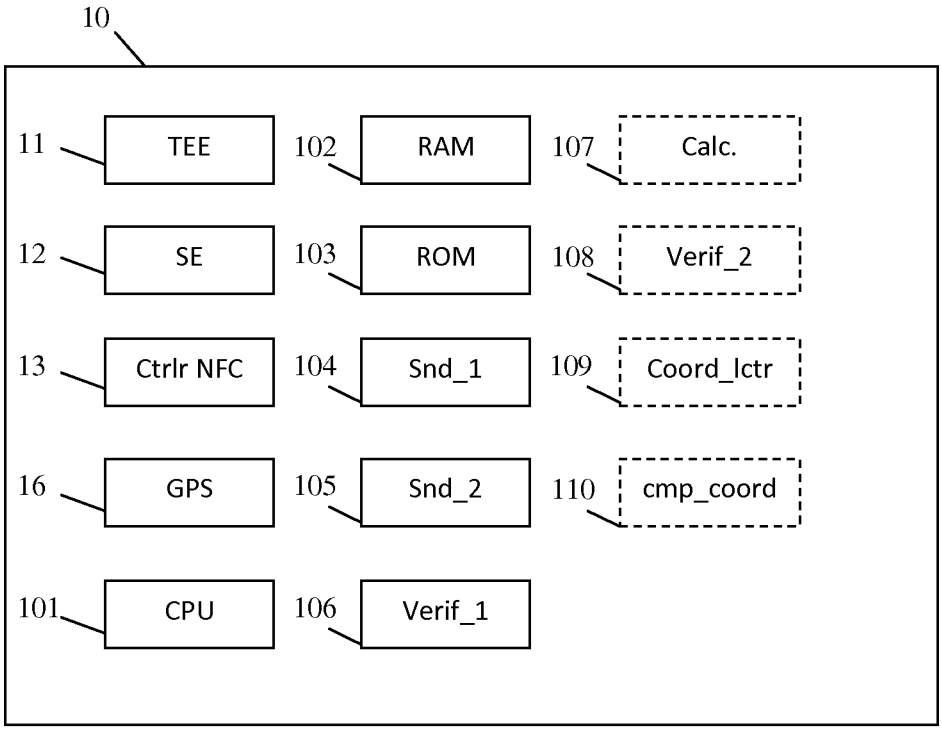

Figure 3

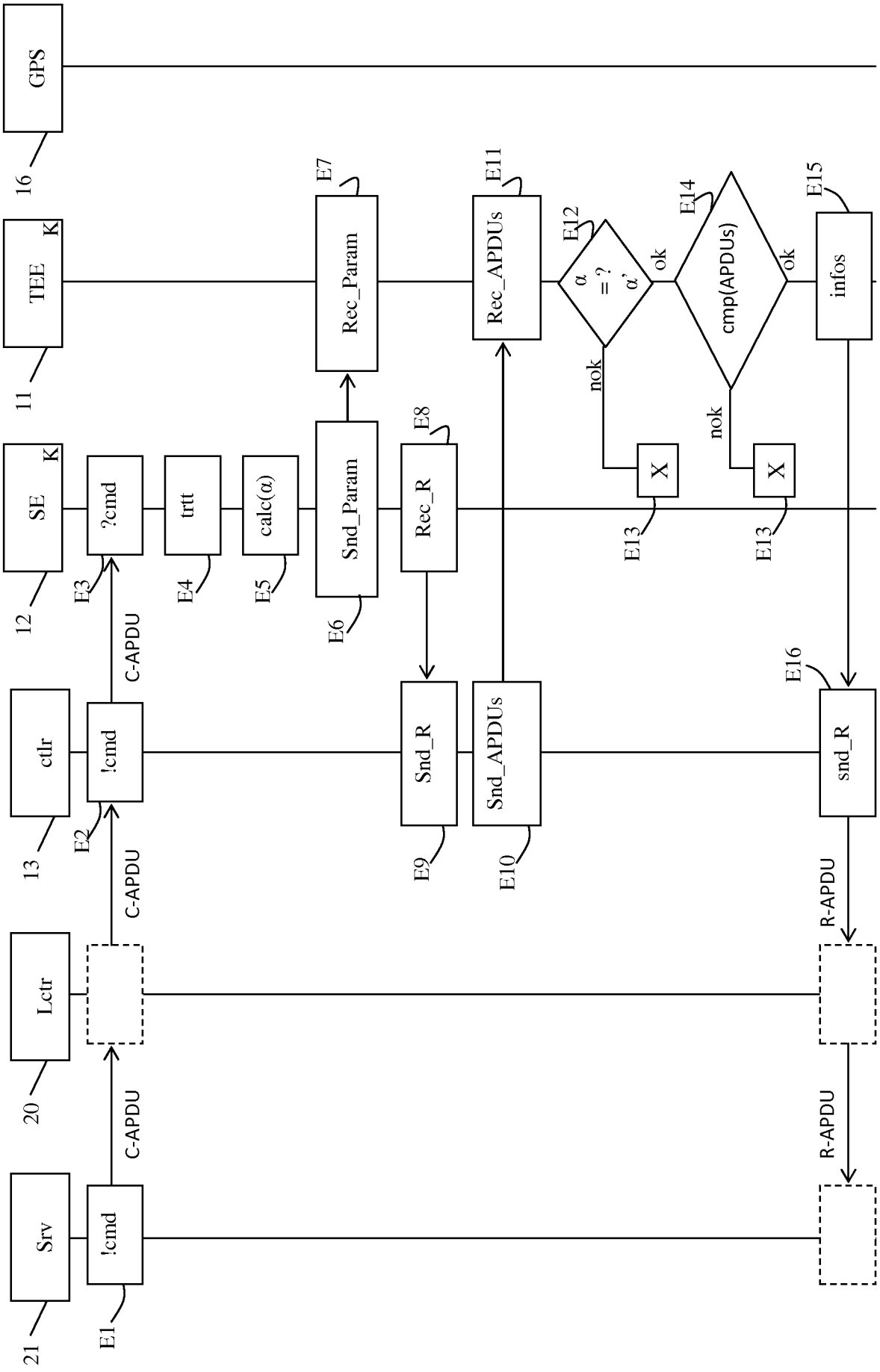
GPS
16
TEE
K
11
SE
K
12
ctlr
13
Lctr
20
Srv
21
?cmd
E3
trtt
E4
calc(α)
E5
Snd_Param
E6
Rec_Param
E7
Rec_R
E8
Snd_R
E9
Snd_APDUs
E10
Rec_APDUs
E11
α = ? α'
E12
ok
nok
X
E13
cmp(APDUs)
E14
ok
nok
X
E13
infos
E15
snd_R
E16
!cmd
E2
C-APDU
!cmd
E1
C-APDU
C-APDU
R-APDU
R-APDU

Figure 2a

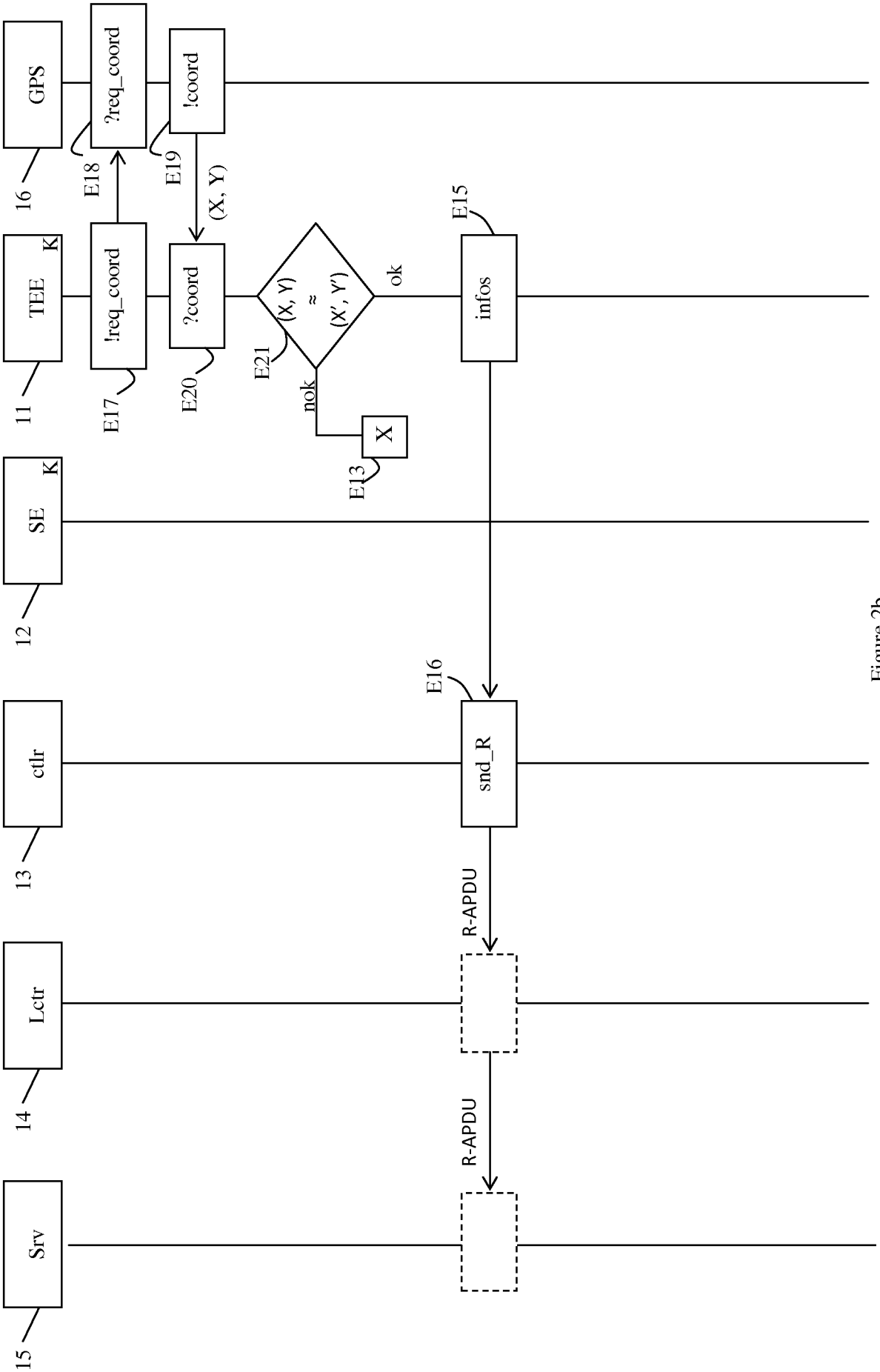
GPS
?req_coord
!coord
16
E18
E19
(X, Y)
TEE
K
!req_coord
?coord
(X, Y) ≈ (X', Y')
ok
nok
E15
infos
11
E17
E20
E21
X
E13
SE
K
12
E16
ctlr
snd_R
13
R-APDU
Lctr
14
R-APDU
Srv
15

Figure 2b

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2015/052579

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/10 H04W12/12
ADD. H04W88/02

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W G06F G06Q

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	Michael Roland: "Software Card Emulation in NFC-enabled Mobile Phones: Great Advantage or Security Nightmare?", , 18 June 2012 (2012-06-18), XP055182749, Retrieved from the Internet: URL:http://www.medien.ifi.lmu.de/iwssi2012/papers/iwssi-spmu2012-roland.pdf [retrieved on 2015-04-14] figures 1,2 page 2 section 3.2 page 4 -----	1-10
A	WO 2013/185889 A1 (GIESECKE & DEVRIENT GMBH [DE]) 19 December 2013 (2013-12-19) figure 2 abstract page 5 ----- -/--	1-10

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of 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	Date of mailing of the international search report
5 January 2016	14/01/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Kufer, Léna

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2015/052579

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	LISHOY FRANCIS ET AL: "Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20120224:103814, 24 February 2012 (2012-02-24), pages 1-16, XP061005717, sections 2.1, 2.2, 4.2.1 -----	1-10

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2015/052579

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2013185889 A1	19-12-2013	DE 102012011729 A1	19-12-2013
		WO 2013185889 A1	19-12-2013

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2015/052579

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04W12/10 H04W12/12
ADD. H04W88/02

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)
H04W G06F G06Q

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	Michael Roland: "Software Card Emulation in NFC-enabled Mobile Phones: Great Advantage or Security Nightmare?", , 18 juin 2012 (2012-06-18), XP055182749, Extrait de l'Internet: URL:http://www.medien.ifi.lmu.de/iwssi2012/papers/iwssi-spmu2012-roland.pdf [extrait le 2015-04-14] figures 1,2 page 2 section 3.2 page 4 -----	1-10
A	WO 2013/185889 A1 (GIESECKE & DEVRIENT GMBH [DE]) 19 décembre 2013 (2013-12-19) figure 2 abrégé page 5 ----- -/--	1-10

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

[X] 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	Date d'expédition du présent rapport de recherche internationale
5 janvier 2016	14/01/2016

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Kufer, Léna

1

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2015/052579

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	LISHOY FRANCIS ET AL: "Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, vol. 20120224:103814, 24 février 2012 (2012-02-24), pages 1-16, XP061005717, sections 2.1, 2.2, 4.2.1 -----	1-10

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2015/052579

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 2013185889 A1	19-12-2013	DE 102012011729 A1	19-12-2013
		WO 2013185889 A1	19-12-2013