(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** **2 999 747**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **12 62367**

(51) Int Cl[8] : ***G 06 F 21/30*** *(2017.01)*

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

(54) PROCEDE DE SECURISATION D'UN DISPOSITIF APTE A COMMUNIQUER AVEC UN LECTEUR SELON DEUX PROTOCOLES D'AUTHENTIFICATION.

(22) **Date de dépôt :** 19.12.12.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 20.06.14 Bulletin 14/25.

(45) **Date de la mise à disposition du public du brevet d'invention :** 04.05.18 Bulletin 18/18.

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

Se reporter à la fin du présent fascicule

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

◯ **Demande(s) d'extension :**

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

(72) **Inventeur(s) :** FERAUD ALBAN.

(73) **Titulaire(s) :** OBERTHUR TECHNOLOGIES Société anonyme.

(74) **Mandataire(s) :** CABINET BEAU DE LOMENIE.

FR 2 999 747 - B1

Arrière-plan de l'invention

La présente invention se situe dans le domaine de la sécurisation de documents incorporant des dispositifs électroniques.

Elle trouve une application privilégiée mais non limitative dans le domaine des documents de voyage communiquant avec un lecteur, ou système d'inspection.

Dans le domaine des documents de voyage, on connait en particulier le protocole de contrôle d'accès BAC (Basic Access Control défini par l'OACI dans le document 9303) apte à permettre l'authentification d'un document de voyage par un lecteur de ce document et à chiffrer les communications entre un microcircuit incorporé dans le document et ce lecteur de ce document afin de protéger l'accès à des données d'authentification et des données sécurisées mémorisées par ce microcircuit, par exemple des données biométriques. Le protocole BAC permet aussi d'assurer l'authenticité et l'intégrité des données échangées entre le lecteur et le microcircuit.

Ce protocole BAC utilise, lors de l'authentification, un mécanisme de cryptographie symétrique. Il s'appuie en outre sur deux clés d'accès dérivées de la zone MRZ (Machine Readable Zone) dont les données sont facilement accessibles et généralement imprimées directement sur le document de voyage, à savoir le numéro du document, sa date d'expiration et la date de naissance du porteur du document. En ce sens, il est relativement peu sécurisé.

Un protocole additionnel EAC (Extended Access Control) a été proposé en 2006 pour les passeports de la zone Schengen dits de deuxième génération. Ce protocole EAC, défini par le German Federal Office for Information Security (BSI) dans le rapport technique TR-03110 conserve le protocole BAC pour l'accès à certaines données dites « données habituelles » et le complète en s'appuyant sur une cryptologie avancée pour protéger de manière forte l'accès aux données biométriques, et notamment l'accès aux empreintes digitales, considérées comme les plus sensibles dans l'Union Européenne.

Le protocole PACE (Password Authenticated Connection Establishment) défini dans le document TR SAC v1.0 (Supplemental Access Control) du 11 novembre 2010 par le comité ISO/IEC JTC1 SC17

WG3/TF5 introduit des sécurités supplémentaires au regard du protocole BAC. En effet, le protocole PACE utilise, lors de la phase d'authentification, un mécanisme de cryptographie asymétrique, et utilise deux clés partagées entre le microcircuit du document et le lecteur, l'une pour le chiffrement des communications, l'autre pour protéger l'intégrité et l'authenticité des données, ces clés n'étant pas dérivées de données de la zone MRZ.

Le protocole PACE devra être implémenté dans tous les documents de voyage émis à partir de fin 2014 ; lorsqu'un document de voyage supportera à la fois le protocole PACE et le protocole BAC, la communication avec le lecteur devra utiliser la technologie PACE, plus sécurisée, si le lecteur supporte lui-même le protocole PACE.

Cependant, pour des raisons de comptabilité ascendantes, au moins pendant toute une période de migration, les protocoles BAC et PACE seront amenés à coexister dans les documents de voyage. On notera que la date à laquelle le protocole BAC ne sera plus implémenté dans les documents de voyage n'est pas définie à ce jour, et que ce protocole sera utilisé pendant dix ans après cette date, les documents de voyage étant généralement valables pendant une telle durée.

On peut penser que la technologie BAC moins sécurisée que la technologie PACE, sera la cible d'attaques visant à mettre en péril l'anonymat et la protection de la vie privée du porteur du document en procédant comme suit :

- 1-attaques par dictionnaire. Ces attaques hors ligne consistent à analyser des enregistrements de transaction obtenus par un attaquant (soit par interception, soit par interaction directe entre le document de voyage et l'attaquant). Elles visent à retrouver la clef statique du document (MRZ) qui est l'identifiant unique du document.
- 2-une fois la MRZ connue :
    - Déterminer si la personne associée à la MRZ est ou était présente à un endroit donné et à un moment donné, en analysant l'enregistrement de transaction électronique interceptée, ou par interaction directe avec le document de voyage via un protocole BAC ou PACE.

- Retrouver les données chiffrées échangées à partir des transactions enregistrées.

Il a en effet été précisé qu'une fois la migration réalisée, c'est-à-dire lorsque les documents de voyage et les lecteurs supporteront le protocole PACE, ce dernier sera utilisé. Mais des personnes mal intentionnées pourront toujours utiliser la fonctionnalité BAC pour obtenir des enregistrements de transaction électronique et enregistrer de telles communications pour tenter de retrouver la MRZ et les données sensibles.

Un des buts de l'invention est de sécuriser les documents de voyage supportant les protocoles BAC et PACE, et éventuellement EAC.

De façon plus générale, un des buts de l'invention est de sécuriser un dispositif apte à communiquer avec un lecteur selon deux protocoles d'authentification, en particulier lorsque ceux-ci présentent des niveaux de sécurisation différents et permettant d'acquérir les même droits d'accès auprès de la puce.

Objet et résumé de l'invention

Plus précisément, l'invention concerne un dispositif électronique comportant :

- des moyens pour mémoriser au moins une donnée sécurisée;
- des moyens pour communiquer avec un lecteur pour la mise en œuvre d'un premier ou d'un deuxième protocole d'authentification, chacun desdits protocoles étant activable et capable d'accéder à ladite au moins une donnée sécurisée ;
- des moyens aptes à bloquer le premier protocole mais pas le deuxième protocole sur réception d'une information.

Autrement dit, et d'une façon générale, l'invention vise un mécanisme permettant de bloquer uniquement l'un des deux protocoles d'authentification, l'autre restant utilisable, chacun de ces protocoles permettant d'accéder à des mêmes données sécurisées mémorisées dans une mémoire du microcircuit.

Le dispositif selon l'invention peut être constitué par un microcircuit (ou puce).

Dans un mode particulier de réalisation, les deux protocoles utilisent la même interface physique, par exemple une interface de communication sans fil, ou une interface de communication sans contact, par exemple de type NFC, par exemple conforme au protocole ISO/IEC 14443.

Dans un mode préféré de réalisation, le dispositif électronique selon l'invention comporte des moyens pour envoyer un message d'erreur audit lecteur sur réception d'une requête dudit lecteur lorsque le premier protocole est bloqué. Cette requête peut par exemple être une requête de défi ou une requête d'authentification mutuelle lors de la tentative de réalisation du protocole d'authentification qui a été bloqué.

Dans un mode particulier de réalisation du dispositif électronique selon l'invention, le premier protocole d'authentification est moins sécurisé que le deuxième protocole d'authentification.

L'invention permet ainsi de bloquer le protocole d'authentification le moins sécurisé, le protocole d'authentification le plus sécurisé restant utilisable.

L'invention vise aussi un document de voyage, par exemple un document d'identité comportant un dispositif électronique tel que mentionné ci-dessus.

Dans un mode particulier de réalisation de l'invention, le premier protocole d'authentification est le protocole BAC et ledit deuxième protocole d'authentification est le protocole PACE, chacun de ces protocoles BAC et PACE permettant d'accéder à des mêmes données sécurisées, par aux données DG1, DG2, DG14, DG15, etc. et Security Object, comme décrit dans le document TR SAC v1.0 (Supplemental Access Control) du 11 novembre 2010 par le comité ISO/IEC JTC1 SC17 WG3/TF5 déjà mentionné.

Dans un mode particulier de réalisation, l'information dont la réception déclenche le blocage du premier protocole représente une commande reçue du lecteur.

Lorsque le dispositif selon l'invention est incorporé dans un document de voyage, la commande précitée peut être émise par une entité ou une personne autorisée par l'entité ayant émis ce document de voyage, par exemple un Etat. La commande peut en particulier être émise

par un douanier qui inspecte le document de voyage lorsque le porteur passe les frontières de cet Etat.

Dans un mode préféré de réalisation, le dispositif électronique selon l'invention comporte des moyens pour authentifier l'émetteur et/ou pour autoriser la commande reçue précitée.

Dans un mode particulier de réalisation, le dispositif électronique selon l'invention comporte des moyens pour stocker une date de référence et l'information dont la réception entraîne le blocage du premier protocole représente une indication relative à la comparaison de cette date de référence avec la date courante.

Ce mode particulier de réalisation permet de bloquer automatiquement l'utilisation du premier protocole à la première utilisation du dispositif survenant après une date de référence mémorisée dans le dispositif.

La date courante peut être reçue du dispositif selon l'invention de différentes façons.

La date peut être comprise dans une commande reçue du lecteur.

Le dispositif selon l'invention peut aussi obtenir la date courante à partir des messages utilisés par protocole différent du premier et second protocoles précités). Par exemple, lorsque le dispositif selon l'invention est incorporé dans un document de voyage, les premier et deuxième protocoles étant les protocoles BAC et PACE, la date courante peut être reçue au cours d'une phase d'authentification conforme au protocole EAC.

Dans un autre mode de réalisation, le dispositif selon l'invention comporte des moyens pour mettre en œuvre un compteur du nombre d'utilisations du premier protocole d'authentification et des moyens pour stocker un nombre d'utilisations seuil. Dans ce mode de réalisation, l'information dont la réception entraîne le blocage du premier protocole représente une indication selon laquelle le nombre d'utilisations du premier protocole d'authentification dépasse le nombre d'utilisations seuil.

Dans un mode particulier de réalisation, le compteur du nombre d'utilisations du premier protocole d'authentification augmente à chaque tentative réussie d'utiliser le premier protocole d'authentification.

Dans un autre mode de réalisation, ce compteur augmente à chaque tentative erronée d'utilisation du premier protocole d'authentification et l'information précitée représente une indication selon

laquelle le nombre de tentatives erronée dépasse un nombre prédéterminé.

Dans un mode particulier de réalisation, le dispositif selon l'invention comporte des moyens aptes à débloquer le premier protocole. Cette caractéristique permet de ne bloquer le premier protocole que de façon temporaire, par exemple lorsqu'on suspecte des attaques mal intentionnées sur le dispositif selon l'invention.

L'invention vise aussi un procédé de sécurisation d'un dispositif électronique comportant des moyens pour mémoriser au moins une donnée sécurisée et des moyens pour communiquer avec un lecteur pour la mise en œuvre d'un premier ou d'un deuxième protocole d'authentification, chacun desdits protocoles étant activable et capable d'accéder à ladite au moins une donnée sécurisée, ce procédé comportant :

- une étape de réception d'une information ; et
- une étape de blocage du premier protocole mais pas du deuxième protocole sur réception de cette information.

Les caractéristiques particulières du procédé de sécurisation selon l'invention sont identiques à celle du dispositif selon l'invention tel que mentionné ci-dessus.

Au vu de ce qui précède, on comprend que l'invention permet en particulier de bloquer l'usage du protocole BAC pour l'authentification du document de voyage, le chiffrement, la protection en intégrité et en authenticité des communications entre un lecteur et le microcircuit de ce document de voyage, et de forcer l'usage du protocole PACE :

- sur réception d'une commande, par exemple une commande APDU ou une commande conforme au protocole ISO/IEC 7816 ou ISO/IEC 14443 ; et/ou
- lorsque la date courante dépasse une date de référence mémorisée dans le document de voyage ; et/ou
- lorsque le protocole BAC ou EAC a été utilisé un nombre de fois prédéterminé ; et/ou
- lorsque le protocole BAC ou EAC a été utilisé avec échec un nombre de fois prédéterminé, ce protocole pouvant éventuellement être débloqué après un nombre prédéterminé d'utilisations réussies du protocole PACE.

Brève description des dessins

D'autres caractéristiques et avantages de la présente invention ressortiront de la description faite ci-dessous, en référence aux dessins annexés qui en illustrent quatre variantes de réalisation dépourvues de tout caractère limitatif. Sur les figures :

- les figures 1A à 1C illustrent une première variante de réalisation de l'invention ;
- les figures 2A à 2C illustrent une deuxième variante de réalisation de l'invention ;
- les figures 3A et 3B illustrent une troisième variante de réalisation de l'invention ; et
- les figures 4A à 4C illustrent une quatrième variante de réalisation de l'invention.

Description détaillée de l'invention

La présente invention va maintenant être décrite dans quatre variantes de réalisation.

a/ Première variante de réalisation de l'invention

La figure 1A représente un document de voyage 101, par exemple un passeport, comportant un microcircuit 102 conforme à une première variante de réalisation de l'invention, ce microcircuit comportant un module 300 apte à mettre en œuvre le protocole BAC et un module 400 apte à mettre en œuvre le protocole PACE pour protéger les communications avec un lecteur 1. Chacun de ces protocoles permet d'accéder à des mêmes données sécurisées DS mémorisées dans une mémoire MEM du microcircuit 102.

Conformément à l'invention, le protocole PACE peut toujours être utilisé mais le protocole BAC peut être bloqué.

A cet effet, le microcircuit 102 comporte une mémoire 200 mémorisant une variable binaire BAC_? pouvant prendre deux valeurs BAC_ON et BAC_OFF, représentant respectivement le fait que le protocole

BAC est utilisable (autrement dit débloqué) ou inutilisable (autrement dit bloqué).

Lorsque le document de voyage est émis, la variable binaire BAC_? est initialisée avec la valeur BAC_ON de sorte que le protocole BAC peut être utilisé.

Dans ce mode de réalisation, le blocage du protocole BAC, autrement dit l'écriture de la valeur BAC_OFF dans la variable binaire BAC_? se fait sur réception d'une commande externe de blocage BLOCK_BAC émise sous le contrôle de l'émetteur du document de voyage, typiquement sous le contrôle d'un fonctionnaire de l'Etat ayant émis le document de voyage.

Cette commande BLOCK_BAC peut par exemple être émise par un douanier qui inspecte le document de voyage au moyen du lecteur 1 lorsque le porteur du document de voyage quitte l'espace Schengen.

Conformément à l'invention, le blocage du protocole BAC n'entraîne pas le blocage du protocole PACE, si bien que le protocole PACE reste utilisable.

Dans le mode de réalisation décrit ici, l'émission de la commande de blocage BLOCK_BAC n'est possible qu'après authentification du fonctionnaire de l'Etat autorisé à émettre cette commande.

Cette authentification peut être mise en œuvre selon différents protocoles.

Dans un premier mode de réalisation représenté à la figure 1B, l'authentification se fait conformément au protocole BAC en utilisant des clés d'authentification secrètes dédiées. Dans ce mode de réalisation l'authentification comporte une étape E10 d'envoi, par le lecteur, d'un défi (Get Challenge) au microcircuit 102 du document de voyage, et une étape E12 d'authentification mutuelle du lecteur et du document de voyage.

Dans un deuxième mode de réalisation représenté à la figure 1C, l'authentification peut être réalisée au cours d'une étape E14 conformément au protocole de type EAC. Dans ce mode de réalisation, l'entité autorisée à modifier la variable BAC_? peut par exemple utiliser une clef racine CVCA (Country Verifying Certification Authority) dédiée à cet usage CVCA ou des certificats CVC (Card Verifiable Certificate) possédant un rôle ID déterminé.

Dans ce premier et dans ce deuxième mode de réalisation, le commande de blocage BLOCK_BAC peut être une commande « PUT DATA » telle que définie par le protocole ISO/IEC 7816-4, envoyée par le lecteur 1 au microcircuit 102 au cours d'une étape E16.

Sur réception d'une telle commande, le microcircuit 102 bloque le protocole BAC (étape E18) de sorte que seul le protocole PACE peut être utilisé.

b/ Deuxième variante de réalisation de l'invention

La figure 2A représente un document de voyage 103, comportant un microcircuit 104 conforme à une autre variante de réalisation de l'invention, ce microcircuit 104 comportant un module 300 apte à mettre en œuvre le protocole BAC et un module 400 apte à mettre en œuvre le protocole PACE pour protéger les communications avec un lecteur 2. Chacun de ces protocoles permet d'accéder à des mêmes données sécurisées DS mémorisées dans une mémoire MEM du microcircuit 104.

Ce microcircuit 104 comporte une mémoire non volatile 121 comportant la date courante CURR_DATE et une mémoire non volatile 122 comportant une date de référence REF_DATE.

Dans cette deuxième variante de réalisation de l'invention, on bloque l'utilisation du protocole BAC si la date courante CURR_DATE dépasse la date de référence REF_DATE.

La mise à jour de la date courante CURR_DATE peut être effectuée de plusieurs façons.

Dans un premier mode de réalisation représenté à la figure 2B, la date courante CURR_DATE est mise à jour (étape E21) avec la date indiquée dans les données transmises au document de voyage lors de la phase d'authentification du protocole EAC (étape E20).

Par exemple, dans ce premier mode de réalisation, on compare directement les dates courante CURR_DATE et de référence REF_DATE, au cours d'une étape E24, afin de déterminer si le protocole BAC peut être utilisé ou s'il doit être bloqué.

Dans un deuxième mode de réalisation représenté à la figure 2C, la date courante CURR_DATE est mise à jour (étape E23) par l'envoi d'une

commande explicite (étape E22), par exemple une commande APDU. On peut par exemple utiliser la commande suivante :

- PUT DATA (INS=CA) comme défini par la norme ISO/IEC 7816-4 ; avec le paramètre P1P2=5F25 (date courante) comme défini par la norme ISO/IEC 7816-6.

Par exemple, dans ce deuxième mode de réalisation de cette deuxième variante, le microcircuit comporte une mémoire non volatile 123 optionnelle comportant une variable binaire BAC2_? pouvant prendre deux valeurs BAC_ON et BAC_OFF, représentant respectivement le fait que le protocole BAC est utilisable (autrement dit débloqué) ou inutilisable (autrement dit bloqué). Lorsque le document de voyage est émis, la variable binaire BAC2_? est initialisée avec la valeur BAC_ON et le protocole BAC peut être utilisé ; la variable binaire BAC2_? prend la valeur BAC_OFF (étape E25) lorsque la date courante CURR_DATE dépasse la date de référence REF_DATE.

La comparaison de la variable binaire BAC2_? avec la valeur BAC_ON (étape E26), ou la comparaison de la date courante CURR_DATE avec la date de référence REF_DATE (étape E24) peut être effectuée au moment de la mise à jour de la date courante CURR_DATE ou lorsque le lecteur cherche à réaliser le protocole BAC.

Ces comparaisons peuvent en particulier être réalisées par le microcircuit 104 sur réception de la commande d'obtention de défi (étape E28, Get Challenge) ou sur réception de la commande d'authentification mutuelle (étape E29, Mutual Authenticate) comme représenté à la figure 2B.

Dans le mode de réalisation décrit ici, lorsqu'il ressort de l'étape E24 ou E26 de comparaison que le protocole BAC doit être bloqué, le protocole BAC est bloqué (étape E23) et un mot d'état d'erreur est retourné à la commande Get Challenge (INS = 84) et/ou Mutual Authenticate (INS = 82) précitée. Ce mot d'état peut par exemple être le code '6A81' ou '6D00' comme décrit dans ISO/IEC 7816-4.

c/ Troisième variante de réalisation de l'invention

La figure 3A représente un document de voyage 105, comportant un microcircuit 106 conforme à une autre variante de réalisation de

l'invention, ce microcircuit 106 comportant un module 300 apte à mettre en œuvre le protocole BAC et un module 400 apte à mettre en œuvre le protocole PACE pour protéger les communications avec un lecteur 3. Chacun de ces protocoles permet d'accéder à des mêmes données sécurisées DS mémorisées dans une mémoire MEM du microcircuit 106.

Ce microcircuit 106 comporte une mémoire non volatile 131 comportant un compteur NB_BAC du nombre d'utilisations du protocole BAC, et une mémoire non volatile 132 comportant une valeur seuil MAX_BAC.

Dans ce mode de réalisation, on bloque l'utilisation du protocole BAC lorsque la variable NB_BAC dépasse la valeur seuil MAX_BAC.

La valeur NB_BAC est initialisée à 0 lorsque le document de voyage est émis et incrémenté d'une unité à chaque utilisation du protocole BAC.

Dans un mode particulier de réalisation représenté à la figure 3B, la variable NB_BAC est incrémentée au cours d'une étape E34 après les étapes E30 de réception des commandes d'obtention de défi (Get Challenge) et E32 d'authentification mutuelle (Mutual Authenticate), telles que définies dans le document 9303 de l'OACI.

Dans un premier mode de réalisation de cette troisième variante, on compare directement le compteur NB_BAC et la valeur seuil MAX_BAC afin de déterminer si le protocole BAC peut être utilisé ou s'il doit être bloqué.

Dans un deuxième mode de réalisation de cette troisième variante, le microcircuit comporte une mémoire non volatile 133 optionnelle comportant une variable binaire BAC3_? pouvant prendre deux valeurs BAC_ON et BAC_OFF, représentant respectivement le fait que le protocole BAC est utilisable (autrement dit débloqué) ou inutilisable (autrement dit bloqué). Lorsque le document de voyage est émis, la variable binaire BAC3_? est initialisée avec la valeur BAC_ON et le protocole BAC peut être utilisé ; la variable binaire BAC3_? prend la valeur BAC_OFF lorsque le compteur NB_BAC dépasse le seuil MAX_BAC.

La comparaison de la variable binaire BAC3_? avec la valeur BAC_ON (premier mode de réalisation), ou la comparaison du nombre d'utilisations du protocole BAC NB_BAC avec le seuil MAX_BAC (deuxième mode de réalisation), référencée E36 dans les deux cas, peut être

effectuée juste après la mise à jour du compteur NB_BAC (étape E34) et/ou lorsque le lecteur cherche à utiliser le protocole BAC.

Comme cela est représenté à la figure 3B, ces comparaisons E36 peuvent en particulier être réalisées par le microcircuit 106 sur réception de la commande d'obtention de défi (étape E30, Get Challenge) ou sur réception de la commande d'authentification mutuelle (étape E32, Mutual Authenticate).

Dans le mode de réalisation décrit ici, lorsqu'il ressort de l'étape E36 de comparaison que le protocole BAC doit être bloqué (étape E38), un mot d'état d'erreur est retourné à la commande d'obtention de défi ou d'authentification mutuelle. Ce mot d'état peut par exemple être le code '6A81' ou '6D00' comme décrit dans ISO/IEC 7816-4.

d/ Quatrième variante de réalisation de l'invention

La figure 4A représente un document de voyage 107, comportant un microcircuit 108 conforme à une autre variante de réalisation de l'invention, ce microcircuit 108 comportant un module 300 apte à mettre en œuvre le protocole BAC et un module 400 apte à mettre en œuvre le protocole PACE pour protéger les communications avec un lecteur 4. Chacun de ces protocoles permet d'accéder à des mêmes données sécurisées DS mémorisées dans une mémoire MEM du microcircuit 108.

Ce microcircuit 108 comporte une mémoire non volatile 141 comportant un compteur NB_BAC_NG du nombre d'utilisations du protocole BAC ayant échouées, une mémoire non volatile 142 comportant un compteur NB_PACE_OK du nombre d'utilisations consécutives du protocole PACE ayant réussies, une mémoire non volatile 143 comportant une valeur seuil MAX_BAC_NG et une mémoire non volatile 144 comportant une valeur seuil MIN_PACE_OK.

Dans cette variante de réalisation, on bloque l'utilisation du protocole BAC lorsque la variable NB_BAC_NG dépasse la valeur seuil MAX_BAC_NG afin de forcer l'utilisation du protocole PACE et on débloque l'utilisation du protocole BAC lorsque la variable NB_PACE_OK dépasse la valeur seuil MIN_PACE_OK.

Les valeurs NB_BAC_NG et NB_PACE_OK sont initialisées à 0 lorsque le document de voyage est émis.

Dans le mode de réalisation décrit à la figure 4B, la variable NB_BAC_NG est incrémentée d'une unité (étape E42) lors d'un échec de l'étape E41 d'authentification mutuelle, cette étape étant consécutive, comme déjà décrit à une étape E40 d'obtention de défi. La variable NB_PACE_OK est alors réinitialisée à zéro.

Lorsque la variable NB_BAC_NG dépasse MAX_BAC_NG (étape E43), on bloque l'usage du protocole BAC forçant ainsi l'usage du protocole PACE (étape E44).

Dans cette variante de réalisation, et comme représenté à la figure 4C, lorsque le protocole PACE est utilisé avec succès (étapes E45 et E46), on incrémente la variable NB_PACE_OK d'une unité et on réinitialise la variable NB_BAC_NG à zéro (étape E47).

Lorsque la variable NB_PACE_OK dépasse MIN_PACE_OK (étape E48) on débloque l'utilisation du protocole BAC (étape E49).

Ainsi, dans cette quatrième variante de réalisation de l'invention, le protocole BAC n'est bloqué que temporairement, afin de détecter et de prévenir des attaques sur le protocole BAC.

REVENDICATIONS

1. Dispositif électronique (102, 104, 106, 108) comportant :
- des moyens (MEM) pour mémoriser au moins une donnée sécurisée (DS) ;
- des moyens pour communiquer avec un lecteur pour la mise en œuvre d'un premier (300) ou d'un deuxième (400) protocole d'authentification, chacun desdits protocoles étant activable et capable d'accéder à ladite au moins une donnée sécurisée ;
- des moyens aptes à bloquer ledit premier protocole mais pas ledit deuxième protocole sur réception d'une information.

2. Dispositif électronique (102, 104, 106, 108) selon la revendication 1, caractérisé en ce qu'il comporte :
- des moyens de réception d'une requête du lecteur, par exemple une requête de défi ou une requête d'authentification mutuelle ; et
- des moyens pour envoyer un message d'erreur audit lecteur, si ledit premier protocole est bloqué.

3. Dispositif électronique (102) selon la revendication 1 ou 2, caractérisé en ce que ladite information représente une commande reçue du lecteur.

4. Dispositif électronique (102) selon la revendication 3, caractérisé en ce qu'il comporte des moyens pour authentifier l'émetteur de ladite commande reçue.

5. Dispositif électronique (104) selon la revendication 1, caractérisé en ce qu'il comporte des moyens (122) pour stocker une date de référence (REF_DATE) et en ce que ladite information représente une indication relative à la comparaison de ladite date de référence avec une date courante (CURR_DATE).

6. Dispositif électronique (104) selon la revendication 5, caractérisé en ce qu'il comporte des moyens pour obtenir la date courante à partir des messages utilisés par un troisième protocole.

7. Dispositif électronique (104) selon la revendication 5, caractérisé en ce qu'il comporte des moyens pour recevoir du lecteur une commande incluant la date courante.

8. Dispositif électronique (106) selon la revendication 1, caractérisé en ce qu'il comporte des moyens pour mettre en œuvre un compteur du nombre d'utilisations du premier protocole d'authentification et des moyens pour stocker un nombre d'utilisations seuil, et en ce que ladite information représente une indication selon laquelle le nombre d'utilisations du premier protocole d'authentification dépasse le nombre d'utilisations seuil.

9. Dispositif électronique (106) selon la revendication 8, caractérisé en ce que le compteur du nombre d'utilisations du premier protocole d'authentification augmente à chaque tentative d'utiliser ledit premier protocole d'authentification.

10. Dispositif électronique (106) selon la revendication 1, caractérisé en ce qu'il comporte des moyens pour mettre en œuvre un compteur augmentant à chaque tentative erronée d'utilisation dudit premier protocole d'authentification et en ce que ladite information représente une indication selon laquelle le nombre des tentatives erronées dépasse un nombre prédéterminé.

11. Dispositif électronique (108) selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comporte des moyens aptes à débloquer ledit premier protocole.

12. Dispositif électronique (102, 104, 106, 108) selon l'une quelconque des revendications précédentes, caractérisé en ce que ledit premier protocole d'authentification est moins sécurisé que ledit deuxième protocole d'authentification.

13. Dispositif électronique (102, 104, 106, 108) selon l'une quelconque des revendications précédentes, caractérisé en ce que ledit premier protocole d'authentification est le protocole Basic Access Control, BAC selon le document 9303 de l'OACI, et ledit deuxième protocole d'authentification est le protocole PACE selon le document TR SAC v1.0 du 11 novembre 2010 de l'OACI.

14. Document de voyage (101, 103, 105, 107) comportant un dispositif électronique (102, 104, 106, 108) selon l'une quelconque des revendications précédentes.

15. Procédé de sécurisation d'un dispositif électronique comportant des moyens pour mémoriser au moins une donnée sécurisée et des moyens pour communiquer avec un lecteur pour la mise en œuvre d'un premier ou d'un deuxième protocole d'authentification, chacun desdits protocoles étant activable et capable d'accéder à ladite au moins une donnée sécurisée, ce procédé comportant :
- une étape de réception d'une information ; et
- une étape de blocage dudit premier protocole mais pas dudit deuxième protocole sur réception de ladite information.

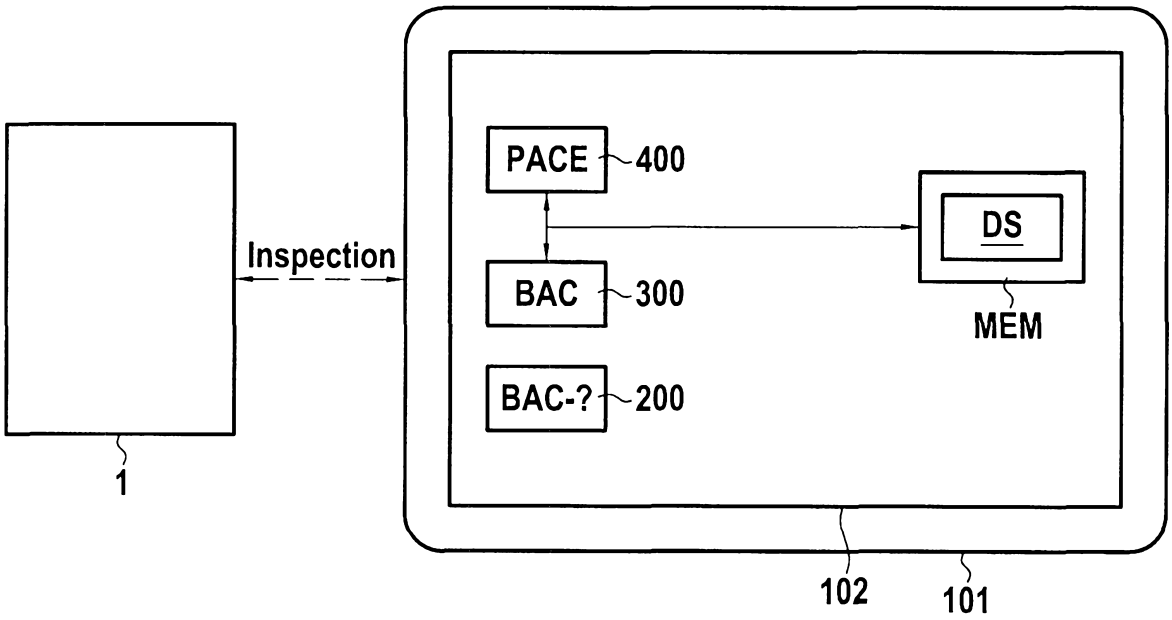

FIG.1A

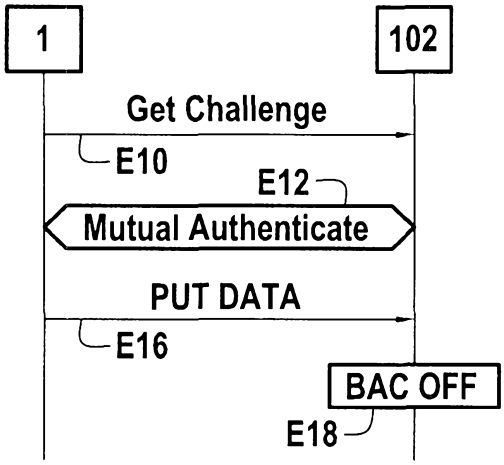

FIG.1B

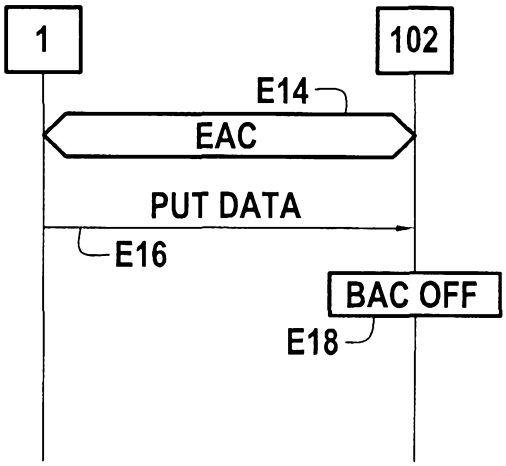

FIG.1C

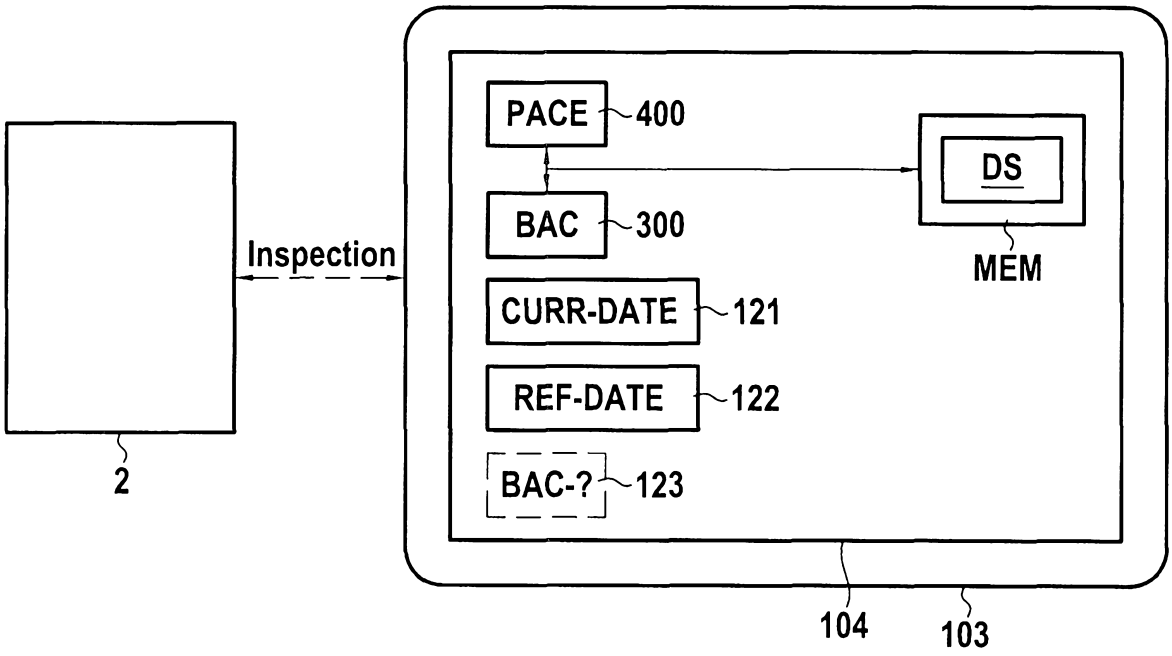
PACE
400
DS
BAC
300
MEM
Inspection
CURR-DATE
121
REF-DATE
122
BAC-?
123
2
104
103

FIG.2A

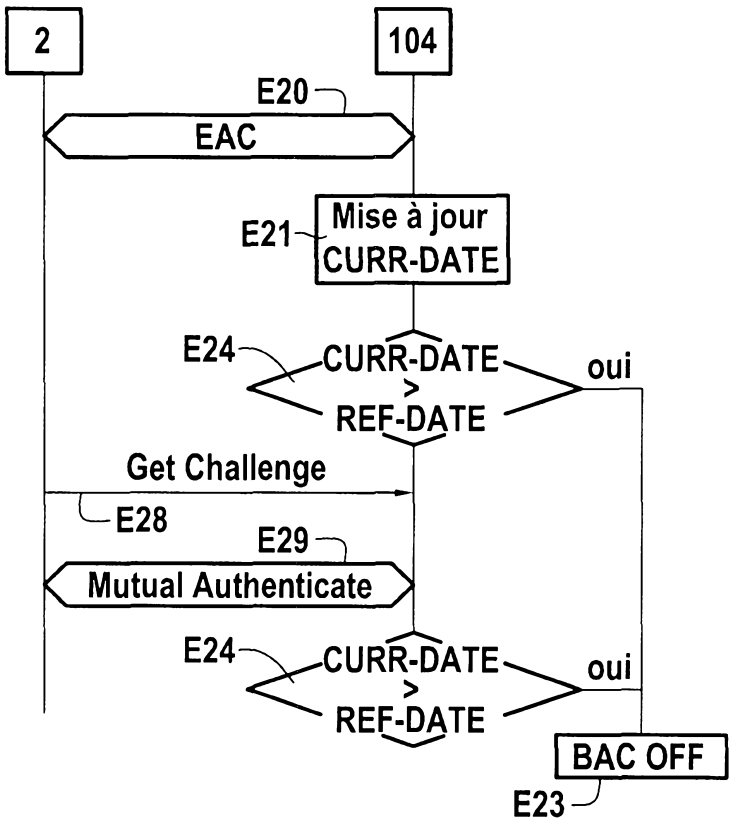
2
104
E20
EAC
E21
Mise à jour
CURR-DATE
E24
CURR-DATE
>
REF-DATE
oui
Get Challenge
E28
E29
Mutual Authenticate
E24
CURR-DATE
>
REF-DATE
oui
BAC OFF
E23

FIG.2B

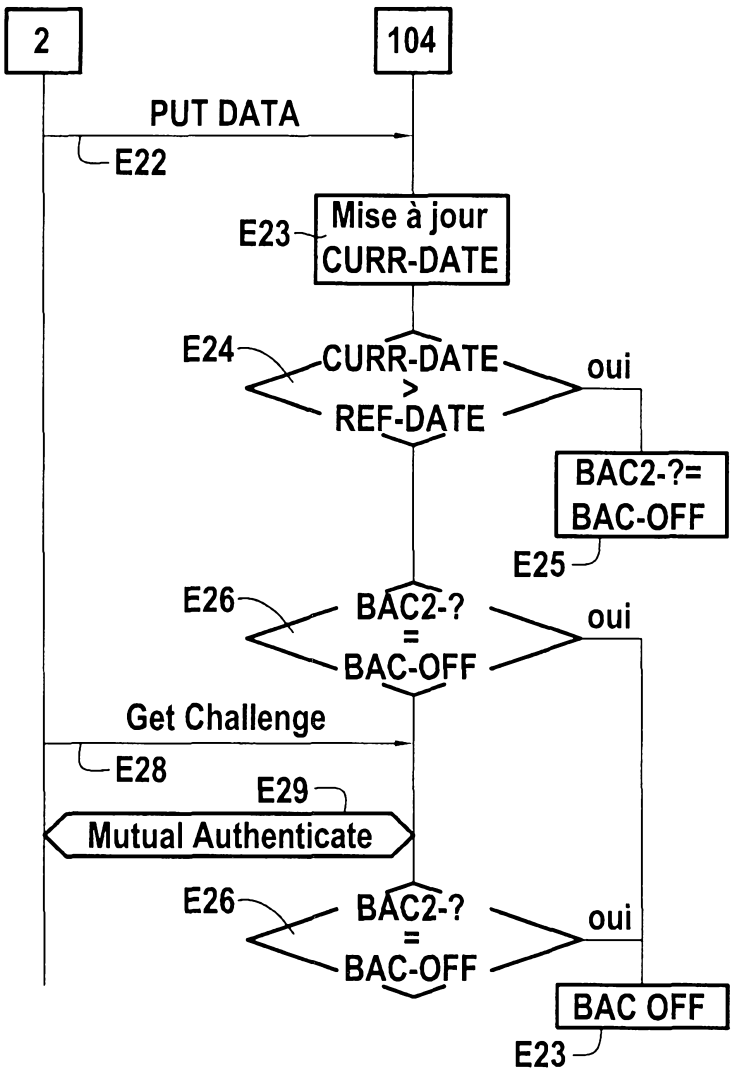
2
104
PUT DATA
E22
E23
Mise à jour
CURR-DATE
E24
CURR-DATE
>
REF-DATE
oui
BAC2-?=
BAC-OFF
E25
E26
BAC2-?
=
BAC-OFF
oui
Get Challenge
E28
E29
Mutual Authenticate
E26
BAC2-?
=
BAC-OFF
oui
BAC OFF
E23

FIG.2C

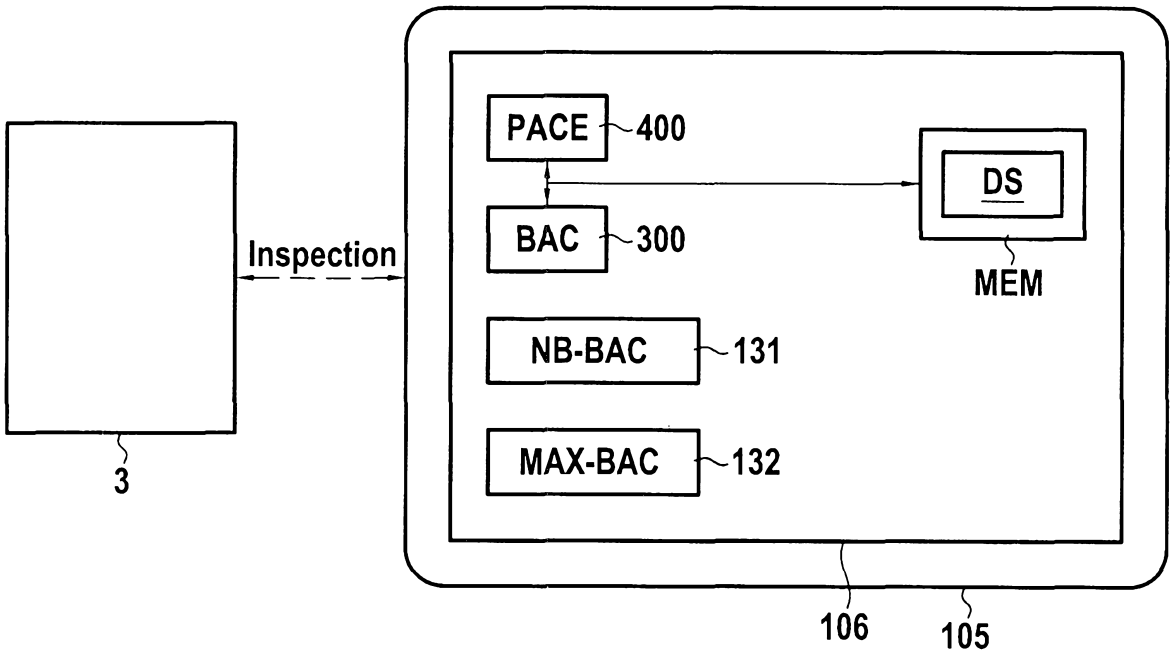
PACE
400
DS
BAC
300
MEM
Inspection
NB-BAC
131
MAX-BAC
132
3
106
105

FIG.3A

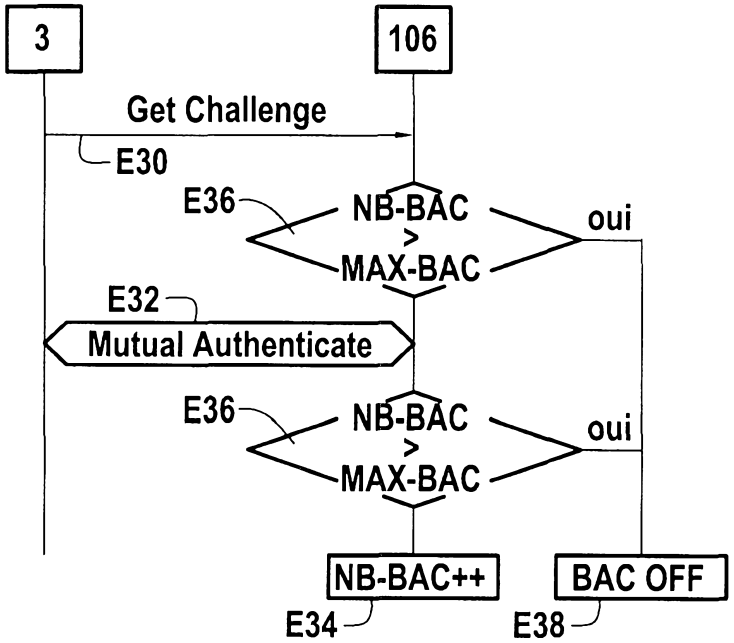
3
106
Get Challenge
E30
E36
NB-BAC
>
MAX-BAC
oui
E32
Mutual Authenticate
E36
NB-BAC
>
MAX-BAC
oui
NB-BAC++
BAC OFF
E34
E38

FIG.3B

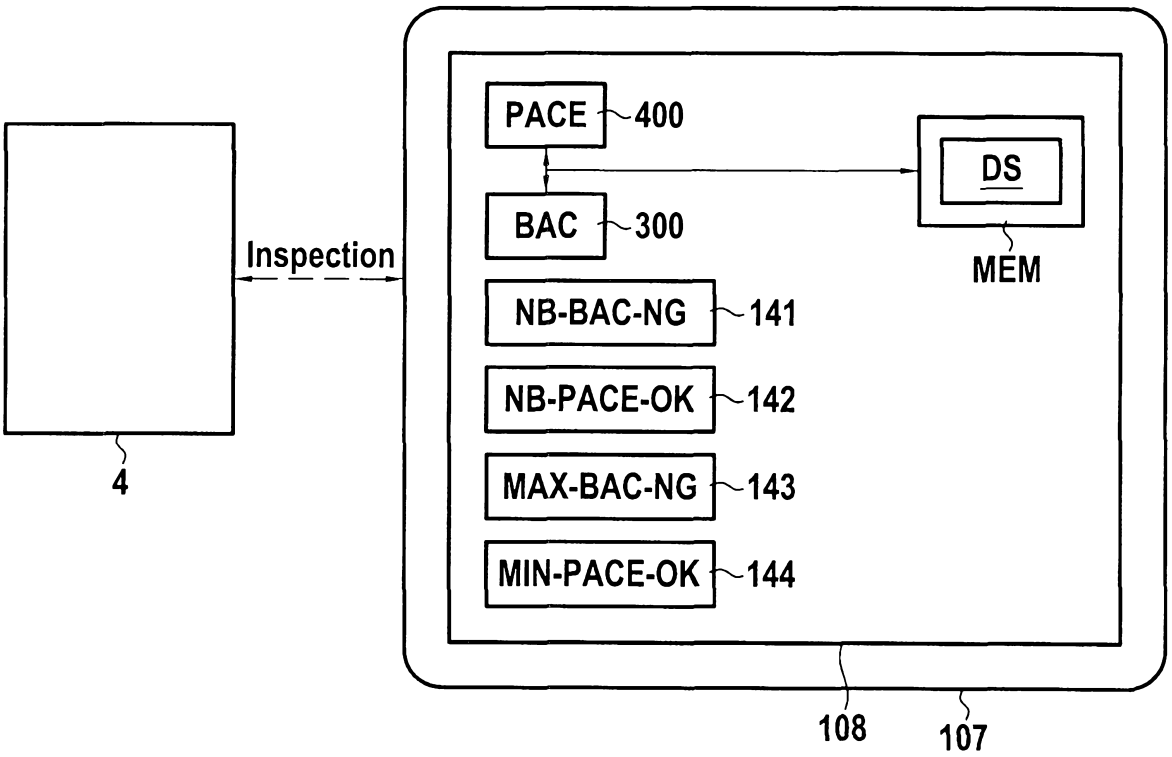
PACE
400
DS
BAC
300
MEM
Inspection
NB-BAC-NG
141
NB-PACE-OK
142
MAX-BAC-NG
143
MIN-PACE-OK
144
4
108
107

FIG.4A

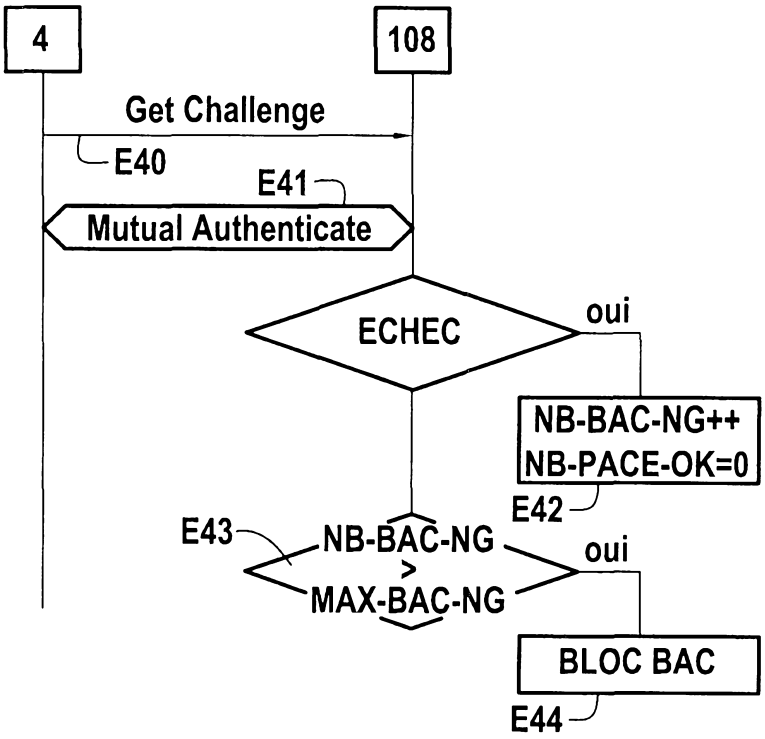
4
108
Get Challenge
E40
E41
Mutual Authenticate
ECHEC
oui
NB-BAC-NG++
NB-PACE-OK=0
E42
E43
NB-BAC-NG
>
MAX-BAC-NG
oui
BLOC BAC
E44

FIG.4B

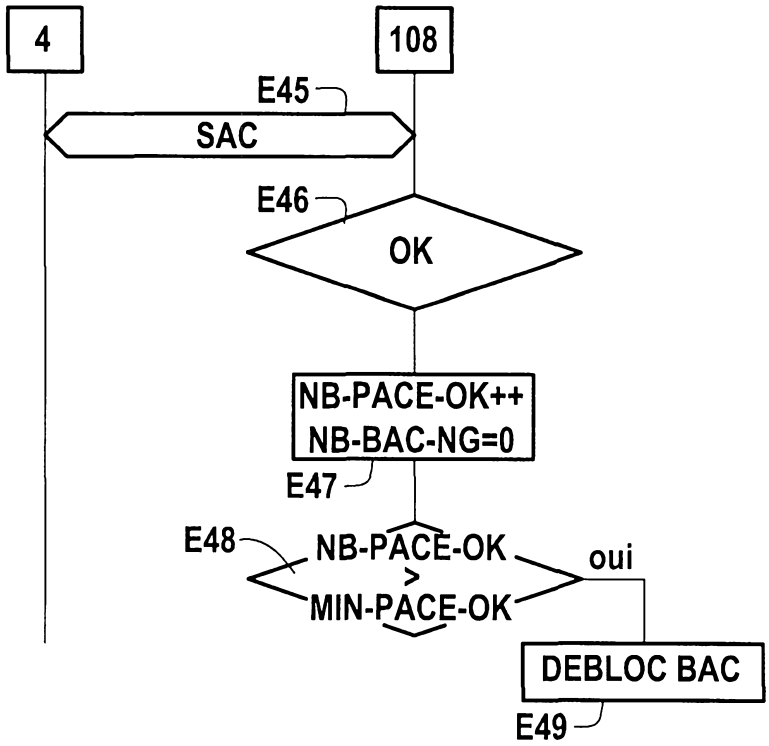
4
108
E45
SAC
E46
OK
NB-PACE-OK++
NB-BAC-NG=0
E47
E48
NB-PACE-OK
>
MIN-PACE-OK
oui
DEBLOC BAC
E49

FIG.4C

N° d'enregistrement national : 1262367 N° de publication : 2999747

RAPPORT DE RECHERCHE

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

OBJET DU RAPPORT DE RECHERCHE

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

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

CONDITIONS D'ÉTABLISSEMENT DU PRÉSENT RAPPORT DE RECHERCHE

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

DOCUMENTS CITÉS DANS LE PRÉSENT RAPPORT DE RECHERCHE

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

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

N° d'enregistrement national : 1262367 N° de publication : 2999747

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

Anonymous: "MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT, Supplemental Access Control forMachine Readable Travel Documents, Version - 1.01", , 11 novembre 2010 (2010-11-11), XP055013829, Extrait de l'Internet: URL:http://www2.icao.int/en/MRTD/Downloads /Technical Reports/Technical Report.pdf [extrait le 2011-12-02]

WO 2008/053095 A1 (OBERTHUR CARD SYST SA [FR]; BERTIN MARC [FR]) 8 mai 2008 (2008-05-08)

EP 1 575 005 A2 (SUN MICROSYSTEMS INC [US]) 14 septembre 2005 (2005-09-14)

EP 0 973 134 A1 (IBM [US]) 19 janvier 2000 (2000-01-19)

WO 2004/032042 A1 (OBERTHUR CARD SYST SA [FR]; JAYET STEPHANE [FR]; HUOT JEAN-CLAUDE [FR]) 15 avril 2004 (2004-04-15)

US 4 879 645 A (TAMADA MASUO [JP] ET AL) 7 novembre 1989 (1989-11-07)

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

NEANT

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

NEANT

N° d'enregistrement national : 1262367 N° de publication : 2999747

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