Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2825050 A1 2012/07/26

(21) 2 825 050

(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2011/12/15
(87) Date publication PCT/PCT Publication Date: 2012/07/26
(85) Entrée phase nationale/National Entry: 2013/07/17
(86) N° demande PCT/PCT Application No.: FR 2011/053009
(87) N° publication PCT/PCT Publication No.: 2012/098306
(30) Priorité/Priority: 2011/01/19 (FR1150415)

(51) Cl.Int./Int.Cl. *H04L 9/32* (2006.01)

(71) Demandeur/Applicant:
NATURAL SECURITY, FR

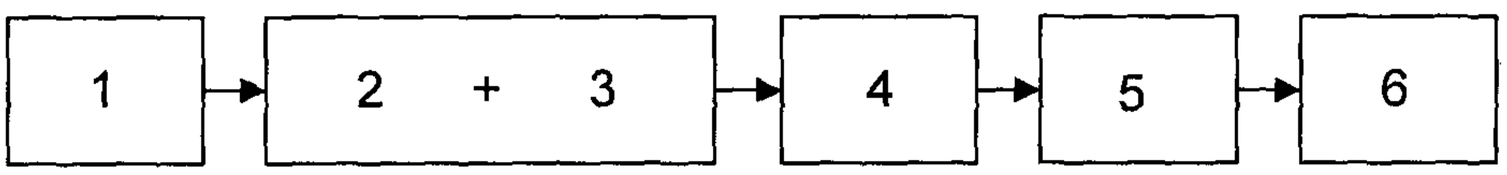
(72) Inventeurs/Inventors:
HOZANNE, CEDRIC, FR;
COUROUBLE, BENOIT, FR

(74) Agent: NORTON ROSE FULBRIGHT CANADA LLP/S.E.N.C.R.L., S.R.L.

(54) Titre : PROCEDE D'AUTHENTIFICATION D'UN PREMIER EQUIPEMENT DE COMMUNICATION PAR UN SECOND EQUIPEMENT DE COMMUNICATION

(54) Title: METHOD FOR AUTHENTICATING FIRST COMMUNICATION EQUIPMENT BY MEANS OF SECOND COMMUNICATION EQUIPMENT

Figure 2



(57) Abrégé/Abstract:
L'invention concerne généralement le domaine des procédés d'authentification biométrique. L'invention concerne plus particulièrement un procédé d'authentification d'un premier équipement de communication par un second équipement de communication. L'invention permet d'atteindre par rapport aux procédés d'authentification biométrique connus de l'art antérieur un gain en nombre d'échanges, et donc en temps, dans la réalisation de l'authentification (2) du premier équipement par le deuxième équipement et l'ouverture (3) d'un canal de communication sécurisé entre ces deux équipements, cette réalisation prenant place dans les procédés d'authentification biométrique entre d'une part une détection (1) du premier équipement par le second, d'autre part une authentification biométrique (5) de l'utilisateur, une sélection d'une application et une transaction applicative entre les deux équipements.

(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
26 juillet 2012 (26.07.2012)

WIPO | PCT

(10) Numéro de publication internationale
WO 2012/098306 A1

(51) Classification internationale des brevets :
H04L 9/32 (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2011/053009

(22) Date de dépôt international :
15 décembre 2011 (15.12.2011)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1150415 19 janvier 2011 (19.01.2011) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **NATURAL SECURITY** [FR/FR]; Euratechnologies, 165 Avenue de Bretagne, F-59000 Lille (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(pour US seulement)* : **HOZANNE, Cédric** [FR/FR]; 73, rue du Beau Rietz, F-62840 Lorgies (FR). **COUROUBLE, Benoît** [FR/FR]; 30 Avenue de Mossley, F-59510 Hem (FR).

(74) Mandataire : **BETHENOD, Marc**; Novagraaf Technologies, 122 rue Edouard Vaillant, F-92593 Levallois-perret cedex (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, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

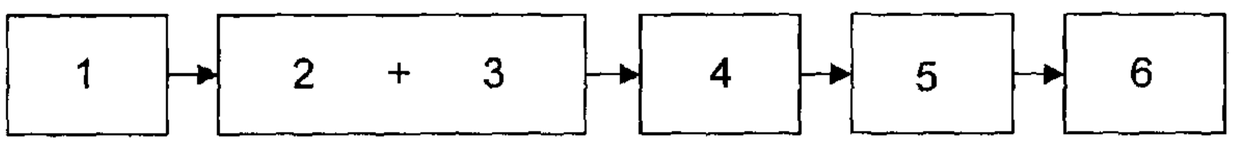
Publiée :

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

(54) **Title** : METHOD FOR AUTHENTICATING FIRST COMMUNICATION EQUIPMENT BY MEANS OF SECOND COMMUNICATION EQUIPMENT

(54) **Titre** : PROCÉDÉ D'AUTHENTIFICATION D'UN PREMIER ÉQUIPEMENT DE COMMUNICATION PAR UN SECOND ÉQUIPEMENT DE COMMUNICATION

Figure 2



(57) **Abstract** : The invention generally relates to the field of biometric authentication methods. The invention specifically relates to a method for authenticating first communication equipment by means of second communication equipment. Compared with the known biometric authentication methods of the prior art, the invention enables an increase to be achieved in the number of exchanges in authenticating (2) the first equipment by means of the second equipment and in opening (3) a secure communication channel between said two pieces of equipment, therefore saving time, said authentication and channel-opening operations taking place in the biometric authentication methods between, on the one hand, a detection (1) of the first equipment by the second equipment, and a biometric authentication (5) of the user and a selection of an application and an application-related transaction between the two pieces of equipment on the other hand.

(57) **Abrégé** : L'invention concerne généralement le domaine des procédés d'authentification biométrique. L'invention concerne plus particulièrement un procédé d'authentification d'un premier équipement de communication par un second équipement de communication. L'invention permet d'atteindre par rapport aux procédés d'authentification biométrique connus de l'art antérieur un gain en nombre d'échanges, et donc en temps, dans la réalisation de l'authentification (2) du premier équipement par le deuxième équipement et l'ouverture (3) d'un canal de communication sécurisé entre ces deux équipements, cette réalisation prenant place dans les

[Suite sur la page suivante]

WO 2012/098306 A1

WO 2012/098306 A1

procédés d'authentification biométrique entre d'une part une détection (1) du premier équipement par le second, d'autre part une authentification biométrique (5) de l'utilisateur, une sélection d'une application et une transaction applicative entre les deux équi - pements.

Procédé d'authentification d'un premier équipement de communication par un second équipement de communication

L'invention concerne généralement le domaine des procédés d'authentification biométrique. L'invention concerne plus particulièrement un procédé d'authentification d'un premier équipement de communication par un second équipement de communication, le premier équipement comprenant au moins un support de mémorisation propre à stocker au moins :

- un énième certificat de chiffrement comprenant une première clé publique associée au premier équipement et une signature apposée par une autorité de certification ayant délivré le certificat de chiffrement, et
- une première clé privée associée asymétriquement à la première clé publique,

le énième certificat de chiffrement étant reconnu par le second équipement.

Les demandes internationales WO 2005/078647 et WO 2007/100709 décrivent des procédés d'authentification biométrique mettant en œuvre au moins un premier équipement de communication et un second équipement de communication. Le premier équipement de communication comprend un moyen de mémorisation pour stocker des données contenant un gabarit biométrique, des applications et des moyens de communication avec et/ou sans contact pour la réception et la transmission de données. Le premier équipement de communication comprend également des moyens de traitement pour opérer notamment une comparaison entre le modèle biométrique qu'il stocke et un échantillon biométrique acquis par un capteur biométrique relié au second équipement de communication et reçu depuis des moyens de communication du second équipement de communication. Si l'échantillon biométrique correspond au modèle biométrique, le porteur du premier équipement de communication est authentifié par le second équipement de communication comme titulaire légitime de cet équipement. Le second équipement de communication est alors

agencé pour compléter l'établissement d'une session transactionnelle avec le premier équipement de communication, puis sélectionner une application du premier équipement de communication à appeler pour compléter la transaction 6 (Cf. figure 1). Le premier équipement de communication est agencé pour transmettre au second équipement de communication un résultat de l'application appelée par le second équipement de communication.

Ces procédés prévoient donc le transfert entre les deux équipements de communication des données biométriques propres à l'utilisateur. On comprend que ce transfert doive être réalisé de façon sécurisée avec des équipements ayant été reconnus intègres et authentiques.

Comme illustré sur la figure 1, postérieurement à une détection 1 avec ou sans contact du premier équipement de communication par le second équipement de communication et préalablement à l'authentification du porteur 4 du premier équipement de communication, ces procédés mettent en œuvre deux étapes successives, distinctes et indépendantes :

- une étape d'authentification 2 du premier équipement de communication par le second équipement de communication, et
- une étape d'ouverture 3 d'un canal de communication sécurisé entre le premier équipement de communication et le second équipement de communication.

Ces deux étapes sont préférentiellement réalisées dans l'ordre susmentionné, de sorte qu'un canal de communication sécurisé ne soit ouvert qu'avec chaque premier équipement de communication authentifié, et il est à noter que l'étape d'ouverture d'un canal de communication sécurisé, quoique présentée comme optionnelle, est préférentiellement réalisée.

Dans ce contexte, et plus particulièrement dans le contexte du

paiement en caisse de marchandises sur un point de vente, on comprend qu'il est avantageux de réduire le temps nécessaire à la réalisation de la transaction.

La présente invention, qui s'appuie sur cette observation originale, propose une solution applicative permettant de réaliser chaque transaction en un temps réduit.

A cette fin, le procédé d'authentification d'un premier équipement de communication par un second équipement de communication, par ailleurs conforme au préambule ci-dessus, est essentiellement tel qu'il comprend :

- une première étape de transmission depuis le premier équipement au second équipement dudit énième certificat de chiffrement,
- une première étape de vérification par le second équipement de la signature dudit énième certificat de chiffrement,
- une première étape de génération par le second équipement d'une première clé de chiffrement, cette dernière comprenant au moins une partie d'un challenge,
- une première étape de chiffrement par le second équipement avec ladite première clé publique de la première clé de chiffrement,
- une deuxième étape de transmission depuis le second équipement au premier équipement de la première clé de chiffrement chiffrée,
- une première étape de déchiffrement par le premier équipement avec ladite première clé privée de ladite première clé de chiffrement chiffrée,
- une deuxième étape de génération par le premier équipement d'une réponse au challenge,
- une troisième étape de transmission depuis le premier équipement au second équipement au moins de la réponse au challenge, et
- une deuxième étape de vérification par le second équipement de la réponse au challenge.

Le procédé permet ainsi de combiner authentification du

premier équipement par le second équipement et ouverture d'un canal de communication sécurisé entre le premier équipement et le second équipement en réduisant significativement le nombre d'échanges nécessaires, et donc le temps nécessaire, par rapport à un procédé dans lequel les étapes d'authentification du premier équipement par le second équipement et d'ouverture d'un canal de communication sécurisé entre le premier équipement et le second équipement sont réalisées de façon successives, distinctes et indépendantes. Il est à noter que la clé de chiffrement est transmise depuis le second équipement au premier équipement de façon sécurisée.

Selon une particularité, le procédé comprend en outre, préalablement à la première étape de transmission depuis le premier équipement au second équipement dudit énième certificat de chiffrement, une première étape de sélection par le second équipement parmi un ensemble de certificats stockés sur le support de mémorisation du premier équipement d'un sous-ensemble de certificats reconnus par le second équipement, ledit sous-ensemble comprenant au moins ledit énième certificat de chiffrement.

Selon une autre particularité, le procédé comprend en outre une deuxième étape de sélection par le second équipement du énième certificat de chiffrement, de sorte que, le certificat de chiffrement étant associé à une méthode de génération d'un canal de communication sécurisé, cette étape de sélection détermine la méthode de génération d'un canal de communication sécurisé à utiliser, chaque méthode de génération d'un canal de communication sécurisé étant associée à un identifiant unique.

Selon un premier mode de réalisation, la première clé de chiffrement est une clé maîtresse de type S-MASTER ou de type S-ENC qui est accompagnée ou non d'une clé de type S-MAC, selon la méthode de génération d'un canal de communication sécurisé utilisée,

et en ce que le challenge compris dans la première clé de chiffrement consiste en un premier identifiant associé à la méthode de génération d'un canal de communication sécurisé utilisée.

Selon une particularité du premier mode de réalisation, le procédé comprend en outre, suite à la première étape de chiffrement par le second équipement avec la première clé publique de la première clé de chiffrement, une troisième étape de génération par le second équipement d'un premier cryptogramme selon un format déterminé, le premier cryptogramme comprenant au moins la première clé de chiffrement chiffrée, la deuxième étape de transmission depuis le second équipement au premier équipement de la première clé de chiffrement chiffrée consistant à transmettre le premier cryptogramme.

Selon une autre particularité du premier mode de réalisation, la deuxième étape de génération par le premier équipement d'une réponse au challenge consiste à générer un second identifiant associé au type de clé maîtresse déchiffrée, la réponse au challenge consistant en le second identifiant.

Selon une autre particularité du premier mode de réalisation, le procédé comprend en outre :

- une deuxième étape de chiffrement par le premier équipement avec la première clé de chiffrement de la réponse au challenge, avant sa transmission depuis le premier équipement au second équipement, et
- une deuxième étape de déchiffrement par le second équipement avec la première clé de chiffrement de la réponse chiffrée, avant sa vérification par le second équipement,

la troisième étape de transmission depuis le premier équipement au second équipement au moins de la réponse au challenge consistant à transmettre au moins la réponse chiffrée au challenge.

Le procédé permet ainsi, avant même la deuxième étape de vérification par le second équipement de la réponse au challenge, c'est-

à-dire avant la fin du procédé selon l'invention, un échange sécurisé par chiffrement/déchiffrement des données transférées d'un équipement à l'autre, tel que le seront les échanges ultérieurs liés à la réalisation d'au moins une transaction.

Selon une autre particularité du premier mode de réalisation, la deuxième étape de vérification par le second équipement de la réponse au challenge consiste en une première étape de comparaison entre les premier et second identifiants.

Selon un deuxième mode de réalisation, la première étape de génération par le second équipement de la première clé de chiffrement comprend une première sous-étape de génération par le second équipement d'un premier nombre aléatoire et une seconde sous-étape de génération d'une seconde clé publique et d'une seconde clé privée asymétriques associées au second équipement, la première clé de chiffrement consistant en un premier ensemble formé par le premier nombre aléatoire et la seconde clé publique, la seconde clé publique constituant ladite au moins une partie du challenge et la seconde clé privée en constituant l'autre partie.

Selon une particularité du deuxième mode de réalisation, le procédé comprend en outre, suite à la première étape de chiffrement par le second équipement avec la première clé publique de la première clé de chiffrement, une troisième étape de génération par le second équipement d'un second cryptogramme selon un format déterminé, le second cryptogramme comprenant au moins la première clé de chiffrement chiffrée, la deuxième étape de transmission depuis le second équipement au premier équipement de la première clé de chiffrement chiffrée consistant à transmettre le second cryptogramme.

Selon une autre particularité du deuxième mode de réalisation, le procédé comprend en outre, après la première étape de

déchiffrement par le premier équipement avec ladite première clé privée de ladite première clé de chiffrement chiffrée, une quatrième étape de génération par le premier équipement d'un second nombre aléatoire, une concaténation des premier et second nombres aléatoires définissant une seconde clé de chiffrement.

Le procédé permet ainsi avantageusement d'atteindre un plus haut niveau de sécurité en ce que la seconde clé de chiffrement, qui sera utilisée ultérieurement pour chiffrer/déchiffrer les échanges entre le premier équipement et le second équipement, est générée en partie par le premier équipement (selon le premier mode de réalisation, la première clé de chiffrement, qui sera celle utilisée ultérieurement pour chiffrer/déchiffrer les échanges entre le premier équipement et le second équipement, est générée uniquement par le second équipement).

Selon une autre particularité du deuxième mode de réalisation, la deuxième étape de génération par le premier équipement de la réponse au challenge consiste en une deuxième étape de chiffrement par le premier équipement avec la seconde clé publique de la seconde clé de chiffrement, la réponse au challenge consistant en la seconde clé de chiffrement chiffrée.

Selon une autre particularité du deuxième mode de réalisation, la deuxième étape de vérification par le second équipement de la réponse au challenge consiste en une troisième étape de déchiffrement par le second équipement avec sa seconde clé privée de la seconde clé de chiffrement chiffrée et en une seconde étape de comparaison entre le premier nombre aléatoire issu de la troisième étape de déchiffrement et le premier nombre aléatoire généré lors de la première étape de génération.

Selon une autre particularité des premier et deuxième modes de réalisation, la réponse au challenge comprend en outre un code

formaté représentatif d'un accusé de réception par le premier équipement de la première clé de chiffrement chiffrée, suite à sa transmission depuis le second équipement, la troisième étape de transmission depuis le premier équipement au second équipement au moins de la réponse au challenge consistant à transmettre en outre ledit code formaté.

Selon une autre particularité des premier et deuxième modes de réalisation, la deuxième étape de vérification par le second équipement de la réponse au challenge consiste en outre à vérifier que le code formaté est représentatif de la bonne réception par le premier équipement de la première clé de chiffrement chiffrée.

Le procédé selon ces deux dernières particularités permet ainsi avantageusement une vérification supplémentaire indépendante de celle liée au challenge soumis au premier équipement par le second équipement.

D'autres caractéristiques et avantages de l'invention ressortiront clairement de la description qui en est faite ci-après, à titre indicatif et nullement limitatif, en référence aux dessins annexés, dans lesquels :

- la figure 1 représente schématiquement un procédé d'authentification biométrique selon l'art antérieur,
- la figure 2 représente schématiquement un procédé d'authentification biométrique tel que mis en œuvre avec le procédé selon l'invention,
- la figure 3 représente schématiquement le procédé selon l'invention,
- la figure 4 représente schématiquement le procédé illustré sur la figure 2 selon un premier mode de réalisation,
- la figure 5 illustre un cryptogramme selon le premier mode de

réalisation du procédé,

- la figure 6 représente schématiquement le procédé illustré sur la figure 2 selon un deuxième mode de réalisation,

- la figure 7 illustre un cryptogramme selon le deuxième mode de réalisation du procédé, et

- la figure 8 illustre le format de la réponse au challenge selon le deuxième mode de réalisation du procédé.

Le procédé d'authentification met en œuvre un premier équipement 10 de communication et un second équipement 20 de communication. Si seule l'authentification du premier équipement par le second est considérée par la suite, il est évident qu'une authentification du second équipement par le premier peut être obtenue, au prix d'une simple inversion de leur rôle respectif dans le présent procédé.

Le second équipement est par exemple un terminal local. Lorsqu'il comprend entre autre des moyens de communication sans fil, il constitue plus particulièrement un dispositif d'acceptation sans fil (ou 'Wireless Acceptance Device' (WAD) selon la terminologie anglaise). Le second équipement de communication est utilisé par un utilisateur dit d'acceptation, tel qu'un marchand, pour réaliser des transactions de services, telles que la vente/l'achat de marchandises ou de services, le retrait d'argent, le paiement par Internet, les opérations de fidélisation, le contrôle d'accès physique, ...

Le second équipement comprend préférentiellement un ensemble de composants, dont :

- un dispositif de réseau personnel sans fil (ou 'Wireless Personal Area Network (WPAN) selon la terminologie anglaise), qui lui fournit la capacité de communiquer sans fil,

- un dispositif d'entrée de données de vérification (ou Verification Data Entry Device (VED) selon la terminologie anglaise),

qui lui permet d'acquérir des données de vérification individuelles (par exemple biométriques) de l'utilisateur, et

- des caractéristiques logicielles de fonctionnement compatibles avec les deux premiers composants.

Le second équipement de communication peut également comprendre une interface homme-machine (ou 'Human-Machine Interface' (HMI) selon la terminologie anglaise) pour indiquer à son utilisateur la progression des transactions.

Le dispositif de réseau personnel sans fil (WPAN) est un composant matériel fournissant au second équipement de communication une interface de réseau personnel sans fil utilisée pour interconnecter des dispositifs se trouvant dans une zone de couverture limitée autour du dispositif de réseau personnel. Le second équipement de communication utilise le protocole du dispositif de réseau personnel pour communiquer, par exemple échanger des données ou des commandes, avec potentiellement une pluralité de premiers équipements de communication présente dans la zone de couverture du dispositif de réseau personnel.

Le dispositif de réseau personnel sans fil est localisé, mais sa localisation n'est pas restreinte. Il peut être embarqué dans le second équipement de communication ou en être séparé et connecté en temps que périphérique, par exemple par une liaison de type USB, à un autre dispositif, par exemple une caisse enregistreuse d'un point de vente.

Le second équipement portable est agencé pour communiquer au moins avec un premier équipement de communication.

Le premier équipement de communication est par exemple un dispositif personnel sans fil (ou Wireless Personal Device (WPD) selon la terminologie anglaise). Il est porté et utilisé par un utilisateur.

Le second équipement de communication est notamment agencé grâce à son dispositif d'entrée de données de vérification pour

capter et transmettre au premier équipement de communication des données individuelles, par exemple biométriques, afin que le premier équipement de communication compare ces données à un gabarit qu'il stocke pour authentifier ou non son utilisateur comme titulaire légitime. Cette étape est illustrée sur la figure 1 et la figure 2 par la référence numérique 4.

Cet exemple d'authentification biométrique de l'utilisateur du premier équipement portable illustre que les premier et second équipements sont agencés pour réaliser une transaction applicative entre eux au cours de ce qu'il convient d'appeler une session transactionnelle.

Une session transactionnelle comprend plus particulièrement :

- une étape d'initialisation de la session, qui consiste à initier la communication entre le second équipement et au moins un premier équipement,

- une étape d'interaction, au cours de laquelle différentes étapes à valeur ajoutée sont réalisées,

- une étape de clôturation de la session, qui clôture la communication entre le second équipement et un premier équipement.

Le modèle de session transactionnelle ci-dessus s'applique quelque soit le mode de communication, par exemple avec ou sans contact. L'utilisation d'un mode de communication particulier n'introduit des spécificités que lors de l'étape d'initialisation et l'étape de clôturation de la session.

Dans un mode de communication sans contact, l'étape d'initialisation se réfère au processus de détection (Cf. la référence 1 sur la figure 1 et la figure 2) par le second équipement de la pluralité de premiers équipements présents dans la zone de couverture du réseau personnel sans fil.

Pendant une session, l'interaction entre le second équipement

de communication et un premier équipement de communication est réalisée par utilisation d'échanges de messages de commandes et de réponses initiés par le second équipement. Les commandes (ou Command - Automatic Data Processing Unit (C-ADPU) selon la terminologie anglaise) et les réponses (ou Response - Automatic Data Processing Unit (C-ADPU) selon la terminologie anglaise) sont basées par exemple sur la norme ISO4. Le transfert des commandes depuis le second équipement à un premier équipement et des réponses depuis un premier équipement au second équipement dépend du mode de communication.

L'étape d'interaction est réalisée indépendamment du mode de communication utilisé. Elle peut comprendre la sélection d'un fournisseur d'accès personnel (ou Personal Acces provider (PAP) selon la terminologie anglaise), qui fournit des services tel que l'authentification du premier équipement (Cf. la référence 2 sur la figure 1 et la figure 2), la création d'un canal de communication sécurisé (Cf. la référence 3 sur la figure 1 et la figure 2) et l'authentification biométrique de l'utilisateur (Cf. la référence 4 sur la figure 1 et la figure 2).

Il est important de noter qu'il est ainsi d'autant plus avantageux de réduire le temps que prend nécessairement l'étape d'interaction du fait que cette étape comprend des étapes d'échanges préalables à toute transaction de service qui sont réalisées pour chaque premier équipement de communication parmi la pluralité de premiers équipements détectés.

L'étape d'interaction consiste également en l'exécution d'une ou plusieurs transactions de service (Cf. les références 5 et 6 sur la figure 1 et la figure 2). Une transaction de service est l'exécution d'une application fournie par un fournisseur de service. Plusieurs transactions de service peuvent être exécutées pendant une même session

transactionnelle, par exemple une transaction de paiement et une opération de fidélisation.

Notamment pour permettre l'authentification du premier équipement de communication par le second équipement de communication, au moins un ensemble de certificats est stocké sur un support de mémorisation du premier équipement, cet ensemble comprenant au moins un certificat d'authentification et/ou de chiffrement. Parmi cet ensemble de certificats, un sous-ensemble de certificats est nécessairement reconnu par le second équipement. Dans le cas contraire, l'authentification du premier équipement de communication par le second équipement de communication ne peut aboutir ; l'authentification échoue et le procédé d'authentification biométrique s'interrompt. Comme illustré sur la figure 4 et la figure 6, le second équipement sélectionne, lors d'une première étape de sélection 100, le sous-ensemble de certificats qu'il reconnaît parmi ledit ensemble. Il est nécessaire en vue d'authentifier le premier équipement que ce sous-ensemble comprenne ledit au moins un certificat d'authentification et/ou de chiffrement.

Dans le cas où plusieurs certificats de chiffrement sont reconnus par le second équipement, le procédé prévoit une deuxième étape de sélection 101, illustrée sur la figure 4 et la figure 6, par le second équipement d'un seul certificat de chiffrement, appelé le énième certificat de chiffrement.

Chaque certificat de chiffrement étant associé à une méthode de génération d'un canal de communication sécurisé, cette étape de sélection 101, ou équivalemment l'étape de sélection 100 dans le cas où elle aboutit à la sélection d'un seul certificat de chiffrement reconnu, détermine la méthode de génération d'un canal de communication sécurisé à utiliser. De plus, chaque méthode de génération d'un canal

de communication sécurisé est associée à un identifiant unique, de sorte que le certificat de chiffrement sélectionné est indirectement associé à un identifiant unique.

Le énième certificat de chiffrement stocké sur le support de mémorisation du premier équipement comprend au moins une première clé publique associée au premier équipement et une signature apposée par une autorité de certification ayant délivré le certificat de chiffrement. Le support de mémorisation du premier équipement stocke également une première clé privée associée asymétriquement à la première clé publique. Il apparaît dès lors que le procédé repose essentiellement sur deux paramètres distincts : un algorithme de chiffrement asymétrique et un schéma de signature numérique.

Comme illustré sur la figure 3, le procédé comprend :

- une première étape de transmission 102 depuis le premier équipement au second équipement dudit énième certificat de chiffrement,
- une première étape de vérification 103 par le second équipement de la signature dudit énième certificat de chiffrement,
- une première étape de génération 104 par le second équipement d'une première clé de chiffrement, cette dernière comprenant au moins une partie d'un challenge,
- une première étape de chiffrement 105 par le second équipement avec ladite première clé publique de la première clé de chiffrement,
- une deuxième étape de transmission 106 depuis le second équipement au premier équipement de la première clé de chiffrement chiffrée,
- une première étape de déchiffrement 107 par le premier équipement avec ladite première clé privée de ladite première clé de chiffrement chiffrée,
- une deuxième étape de génération 108 par le premier équipement

d'une réponse au challenge,

- une troisième étape de transmission 109 depuis le premier équipement au second équipement au moins de la réponse au challenge, et
- une deuxième étape de vérification 110 par le second équipement de la réponse au challenge.

Le procédé permet ainsi de combiner authentification du premier équipement par le second équipement et ouverture d'un canal de communication sécurisé entre le premier équipement et le second équipement en réduisant significativement le nombre d'échanges nécessaires, et donc le temps nécessaire, par rapport à un procédé dans lequel les étapes d'authentification du premier équipement par le second équipement et d'ouverture d'un canal de communication sécurisé entre le premier équipement et le second équipement sont réalisées de façon successives, distinctes et indépendantes. Plus particulièrement, seules trois étapes dites de transmission sont nécessaires à l'obtention du résultat désiré atteint. Il est à noter, de plus, que la clé de chiffrement est transmise depuis le second équipement au premier équipement de façon sécurisée, car, étant chiffrée avec ladite clé publique du premier équipement, seul ce dernier peut la déchiffrer avec sa clé privée.

Par ailleurs, il est à noter que la première étape de vérification 103 par le second équipement de la signature dudit énième certificat de chiffrement, si elle ne renvoie pas un résultat positif, induit l'échec de l'authentification et l'interruption du procédé d'authentification biométrique.

Il doit être entendu que les premier et second équipements comprennent des moyens de traitement pour vérifier, chiffrer et/ou déchiffrer.

La première étape de vérification 103 par le second équipement

de la signature dudit énième certificat de chiffrement est réalisée en utilisant un algorithme de vérification associé utilisé conjointement avec la clé publique de l'autorité de certification correspondante et le schéma de signature numérique correspondant.

Le procédé se décline plus particulièrement sous deux modes de réalisation qui mettent en œuvre de façon différentes certaines des étapes du procédé présenté ci-dessus. Les deux modes de réalisation du procédé vont plus particulièrement être décrits ci-dessous.

Le premier mode de réalisation du procédé est illustré sur la figure 4 et la figure 5.

Selon le premier mode de réalisation du procédé et comme plus particulièrement illustré sur la figure 5, la première clé de chiffrement est une clé maîtresse de type S-MASTER 70 ou de type S-ENC 71 selon la méthode de génération d'un canal de communication sécurisé utilisée. Cette clé maîtresse est accompagnée ou non d'une clé de type S-MAC 72 selon la méthode de génération d'un canal de communication sécurisé utilisée. Le challenge compris dans la première clé de chiffrement consiste en un premier identifiant 73 associé à la méthode de génération d'un canal de communication sécurisé utilisée.

Selon le premier mode de réalisation, le procédé comprend en outre, suite à la première étape de chiffrement 105 par le second équipement avec la première clé publique de la première clé de chiffrement, une troisième étape de génération 1051 par le second équipement d'un premier cryptogramme 74 selon un format déterminé. Comme illustré sur la figure 6, le premier cryptogramme comprend au moins la première clé de chiffrement chiffrée 70, 71 ou 72. La deuxième étape de transmission 106 depuis le second équipement au premier équipement de la première clé de chiffrement chiffrée consiste alors à

transmettre le premier cryptogramme.

Selon le premier mode de réalisation, la deuxième étape de génération 108 par le premier équipement d'une réponse au challenge consiste à générer un second identifiant associé au type de clé maîtresse déchiffrée. La réponse au challenge consiste alors précisément en le second identifiant. Ainsi, lors de l'étape de sélection 100 ou 101, le second équipement a sélectionné un certificat associé à un identifiant, cet identifiant est compris dans la clé de chiffrement et est chiffré avec celle-ci. Puis, le premier équipement déchiffre avec sa clé privée la première clé de chiffrement et récupère notamment ledit identifiant. Cet identifiant s'il est déchiffré avec la première clé privée du premier équipement ayant transmis son certificat de chiffrement doit correspondre à l'identifiant associé à la méthode de génération d'un canal de communication sécurisé définie dans le certificat de chiffrement. Le challenge a ainsi été défini par le second équipement sur la base de données propres à la méthode de génération d'un canal de communication sécurisé, puis soumis au premier équipement qui d'une part est le seul à pouvoir en déchiffrer la réponse et d'autre part connaît *a priori* la réponse *ad hoc* au challenge. Il est à noter qu'indépendamment l'identifiant 73 (Cf. figure 6) de la méthode de génération d'un canal de communication sécurisé utilisée peut être écrite de façon non chiffrée dans le premier cryptogramme.

Selon le premier mode de réalisation, le procédé comprend en outre :

- une deuxième étape de chiffrement par le premier équipement avec la première clé de chiffrement de la réponse au challenge, avant sa transmission depuis le premier équipement au second équipement, et
- une deuxième étape de déchiffrement par le second équipement avec la première clé de chiffrement de la réponse chiffrée, avant sa vérification par le second équipement. La troisième étape de

transmission 109 depuis le premier équipement au second équipement de la réponse au challenge consiste alors à transmettre au moins la réponse chiffrée au challenge.

Selon le premier mode de réalisation, le procédé prévoit donc avantageusement, avant même la deuxième étape de vérification par le second équipement de la réponse au challenge, un échange sécurisé par chiffrement/déchiffrement des données transférées d'un équipement à l'autre, tel que le seront les échanges ultérieurs liés à la réalisation d'au moins une transaction de service.

Selon le premier mode de réalisation, la deuxième étape de vérification 110 par le second équipement de la réponse au challenge consiste en une première étape de comparaison entre les premier et second identifiants. La deuxième étape de vérification 110, si elle ne renvoie pas un résultat positif, induit l'échec de l'authentification et l'interruption du procédé d'authentification biométrique ; au contraire, si elle renvoie un résultat positif, elle induit la réussite de l'authentification et la possibilité de poursuivre le procédé d'authentification biométrique, par exemple par une étape d'authentification biométrique de l'utilisateur du premier équipement.

Le deuxième mode de réalisation du procédé est illustré par la figure 6, la figure 7 et la figure 8.

Selon le deuxième mode de réalisation et comme illustré sur la figure 6, la première étape de génération 104 par le second équipement de la première clé de chiffrement comprend une première sous-étape de génération 1041 par le second équipement d'un premier nombre aléatoire 80 et une seconde sous-étape de génération 1042 d'une seconde clé publique 81 et d'une seconde clé privée asymétriques associées au second équipement. La première clé de chiffrement consiste en un premier ensemble formé par le premier nombre aléatoire

et la seconde clé publique. La seconde clé publique constitue ladite au moins une partie du challenge et la seconde clé privée en constitue l'autre partie.

Selon le deuxième mode de réalisation, le procédé comprend en outre, suite à la première étape de chiffrement 105 par le second équipement avec la première clé publique de la première clé de chiffrement, une troisième étape de génération 1052 par le second équipement d'un second cryptogramme 82 selon un format déterminé. Comme illustré sur la figure 7, le second cryptogramme comprend au moins la première clé de chiffrement chiffrée. La deuxième étape de transmission 106 depuis le second équipement au premier équipement de la première clé de chiffrement chiffrée consiste alors à transmettre le second cryptogramme.

Selon le deuxième mode de réalisation et comme illustré sur la figure 6, le procédé comprend en outre, après la première étape de déchiffrement 107 par le premier équipement avec ladite première clé privée de ladite première clé de chiffrement chiffrée, une quatrième étape de génération 1071 par le premier équipement d'un second nombre aléatoire 83 (Cf. figure 8), une concaténation des premier et second nombres aléatoires définissant une seconde clé de chiffrement.

Selon son deuxième mode de réalisation, le procédé permet ainsi avantageusement d'atteindre un plus haut niveau de sécurité en ce que la seconde clé de chiffrement, qui sera celle utilisée ultérieurement pour chiffrer/déchiffrer les échanges entre le premier équipement et le second équipement, est générée en partie par le premier équipement. Au contraire, selon le premier mode de réalisation, la première clé de chiffrement, qui sera celle utilisée ultérieurement pour chiffrer/déchiffrer les échanges entre le premier équipement et le second équipement, est générée uniquement par le second équipement.

Selon le deuxième mode de réalisation, la deuxième étape de génération 108 par le premier équipement de la réponse au challenge consiste en une deuxième étape de chiffrement 1081 par le premier équipement avec la seconde clé publique de la seconde clé de chiffrement. Comme illustré sur la figure 8, la réponse au challenge 84 consiste alors en la seconde clé de chiffrement chiffrée.

Selon le deuxième mode de réalisation et comme illustré sur la figure 6, la deuxième étape de vérification 110 par le second équipement de la réponse au challenge consiste en une troisième étape de déchiffrement 1101 par le second équipement avec sa seconde clé privée de la seconde clé de chiffrement chiffrée et en une seconde étape de comparaison 1102 entre le premier nombre aléatoire issu de la troisième étape de déchiffrement et le premier nombre aléatoire généré lors de la première étape de génération 104.

Comme illustré sur la figure 5 et la figure 7, le premier cryptogramme 74 et le second cryptogramme 82 comprennent en outre plusieurs champs dont un champ pour renseigner une classe (CLA), un champ pour renseigner un premier paramètre (P1), un champ pour renseigner un second paramètre (P2), un champ pour renseigner une longueur du champ de données de commande (Lc), et un champ pour renseigner un identifiant de l'ensemble de certificats sélectionnés reconnus par le second équipement.

Selon le premier mode de réalisation et le second mode de réalisation, la réponse au challenge comprend en outre un code formaté représentatif d'un accusé de réception par le premier équipement de la première clé de chiffrement chiffrée, suite à sa transmission depuis le second équipement. La troisième étape de transmission 109 depuis le premier équipement au second équipement

au moins de la réponse au challenge consiste alors à transmettre en outre ledit code formaté.

Conséquemment, la deuxième étape de vérification 110 par le second équipement de la réponse au challenge consiste en outre à vérifier que le code formaté est représentatif de la bonne réception par le premier équipement de la première clé de chiffrement chiffrée.

Il doit être évident pour les personnes versées dans l'art que la présente invention permet des modes de réalisation sous de nombreuses autres formes spécifiques sans l'éloigner du domaine d'application de l'invention comme revendiqué. Par conséquent, les présents modes de réalisation doivent être considérés à titre d'illustration mais peuvent être modifiés dans le domaine défini par la portée des revendications jointes.

REVENDICATIONS

1. Procédé d'authentification d'un premier équipement (10) de communication par un second équipement (20) de communication, le premier équipement comprenant au moins un support de mémorisation propre à stocker au moins :

- un énième certificat de chiffrement comprenant une première clé publique associée au premier équipement et une signature apposée par une autorité de certification ayant délivré le certificat de chiffrement, et
- une première clé privée associée asymétriquement à la première clé publique,

le énième certificat de chiffrement étant reconnu par le second équipement, le procédé étant caractérisé en ce qu'il comprend :

- une première étape de transmission (102) depuis le premier équipement au second équipement dudit énième certificat de chiffrement,
- une première étape de vérification (103) par le second équipement de la signature dudit énième certificat de chiffrement,
- une première étape de génération (104) par le second équipement d'une première clé de chiffrement, cette dernière comprenant au moins une partie d'un challenge,
- une première étape de chiffrement (105) par le second équipement avec ladite première clé publique de la première clé de chiffrement,
- une deuxième étape de transmission (106) depuis le second équipement au premier équipement de la première clé de chiffrement chiffrée,
- une première étape de déchiffrement (107) par le premier équipement avec ladite première clé privée de ladite première clé de chiffrement chiffrée,
- une deuxième étape de génération (108) par le premier équipement d'une réponse au challenge,

- une troisième étape de transmission (109) depuis le premier équipement au second équipement au moins de la réponse au challenge, et
- une deuxième étape de vérification (110) par le second équipement de la réponse au challenge.

2. Procédé d'authentification selon la revendication 1, caractérisé en ce qu'il comprend en outre, préalablement à la première étape de transmission (102) depuis le premier équipement au second équipement dudit énième certificat de chiffrement, une première étape de sélection (100) par le second équipement parmi un ensemble de certificats stockés sur le support de mémorisation du premier équipement d'un sous-ensemble de certificats reconnus par le second équipement, ledit sous-ensemble comprenant au moins ledit énième certificat de chiffrement.

3. Procédé d'authentification selon la revendication 2, caractérisé en ce que, le procédé comprend en outre une deuxième étape de sélection (101) par le second équipement du énième certificat de chiffrement, de sorte que, le certificat de chiffrement étant associé à une méthode de génération d'un canal de communication sécurisé, cette étape de sélection détermine la méthode de génération d'un canal de communication sécurisé à utiliser, chaque méthode de génération d'un canal de communication sécurisé étant associée à un identifiant unique.

4. Procédé d'authentification selon l'une quelconque des revendications 1 à 3, caractérisé en ce que, la première clé de chiffrement est une clé maîtresse de type S-MASTER (70) ou de type S-ENC (71) qui est accompagnée ou non d'une clé de type S-MAC (72), selon la méthode de génération d'un canal de communication sécurisé utilisée, et en ce

que le challenge compris dans la première clé de chiffrement consiste en un premier identifiant (73) associé à la méthode de génération d'un canal de communication sécurisé utilisée.

5. Procédé d'authentification selon la revendication 4, caractérisé en ce qu'il comprend en outre, suite à la première étape de chiffrement (105) par le second équipement avec la première clé publique de la première clé de chiffrement, une troisième étape de génération (1051) par le second équipement d'un premier cryptogramme (74) selon un format déterminé, le premier cryptogramme comprenant au moins la première clé de chiffrement chiffrée, la deuxième étape de transmission (106) depuis le second équipement au premier équipement de la première clé de chiffrement chiffrée consistant à transmettre le premier cryptogramme.

6. Procédé d'authentification selon la revendication 4 ou la revendication 5, caractérisé en ce que la deuxième étape de génération (108) par le premier équipement d'une réponse au challenge consiste à générer un second identifiant associé au type de clé maîtresse déchiffrée, la réponse au challenge consistant en le second identifiant.

7. Procédé d'authentification selon la revendication 6, caractérisé en ce qu'il comprend en outre :
- une deuxième étape de chiffrement par le premier équipement avec la première clé de chiffrement de la réponse au challenge, avant sa transmission depuis le premier équipement au second équipement, et
- une deuxième étape de déchiffrement par le second équipement avec la première clé de chiffrement de la réponse chiffrée, avant sa vérification par le second équipement,
la troisième étape de transmission (109) depuis le premier équipement

au second équipement au moins de la réponse au challenge consistant à transmettre au moins la réponse chiffrée au challenge.

8. Procédé d'authentification selon la revendication 6 ou la revendication 7, caractérisé en ce que la deuxième étape de vérification (110) par le second équipement de la réponse au challenge consiste en une première étape de comparaison entre les premier et second identifiants.

9. Procédé d'authentification selon l'une quelconque des revendications 1 à 3, caractérisé en ce que la première étape de génération (104) par le second équipement de la première clé de chiffrement comprend une première sous-étape de génération (1041) par le second équipement d'un premier nombre aléatoire (80) et une seconde sous-étape de génération (1042) d'une seconde clé publique (81) et d'une seconde clé privée asymétriques associées au second équipement, la première clé de chiffrement consistant en un premier ensemble formé par le premier nombre aléatoire et la seconde clé publique, la seconde clé publique constituant ladite au moins une partie du challenge et la seconde clé privée en constituant l'autre partie.

10. Procédé d'authentification selon la revendication 9, caractérisé en ce qu'il comprend en outre, suite à la première étape de chiffrement (105) par le second équipement avec la première clé publique de la première clé de chiffrement, une troisième étape de génération (1052) par le second équipement d'un second cryptogramme (82) selon un format déterminé, le second cryptogramme comprenant au moins la première clé de chiffrement chiffrée, la deuxième étape de transmission (106) depuis le second équipement au premier équipement de la première clé de chiffrement chiffrée consistant à transmettre le second

cryptogramme.

11. Procédé d'authentification selon la revendication 9 ou la revendication 10, caractérisé en ce qu'il comprend en outre, après la première étape de déchiffrement (107) par le premier équipement avec ladite première clé privée de ladite première clé de chiffrement chiffrée, une quatrième étape de génération (1071) par le premier équipement d'un second nombre aléatoire (83), une concaténation des premier et second nombres aléatoires définissant une seconde clé de chiffrement.

12. Procédé d'authentification selon la revendication 11, caractérisé en ce que la deuxième étape de génération (108) par le premier équipement de la réponse au challenge consiste en une deuxième étape de chiffrement (1081) par le premier équipement avec la seconde clé publique de la seconde clé de chiffrement, la réponse au challenge (84) consistant en la seconde clé de chiffrement chiffrée.

13. Procédé d'authentification selon la revendication 12, caractérisé en ce que la deuxième étape de vérification (110) par le second équipement de la réponse au challenge consiste en une troisième étape de déchiffrement (1101) par le second équipement avec sa seconde clé privée de la seconde clé de chiffrement chiffrée et en une seconde étape de comparaison (1102) entre le premier nombre aléatoire issu de la troisième étape de déchiffrement et le premier nombre aléatoire généré lors de la première étape de génération (104).

14. Procédé d'authentification selon la revendication 6 ou la revendication 12, caractérisé en ce que la réponse au challenge comprend en outre un code formaté représentatif d'un accusé de réception par le premier équipement de la première clé de chiffrement

chiffrée, suite à sa transmission depuis le second équipement, la troisième étape de transmission (109) depuis le premier équipement au second équipement au moins de la réponse au challenge consistant à transmettre en outre ledit code formaté.

15. Procédé d'authentification selon l'une des revendications 8 et 13, et selon la revendication 14, caractérisé en ce que la deuxième étape de vérification (110) par le second équipement de la réponse au challenge consiste en outre à vérifier que le code formaté est représentatif de la bonne réception par le premier équipement de la première clé de chiffrement chiffrée.

Figure 1

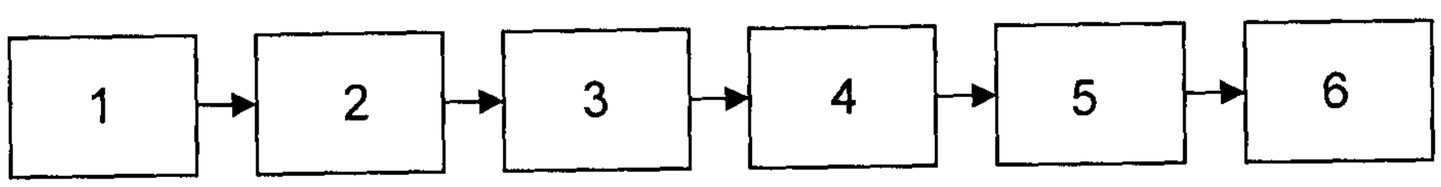


Figure 2

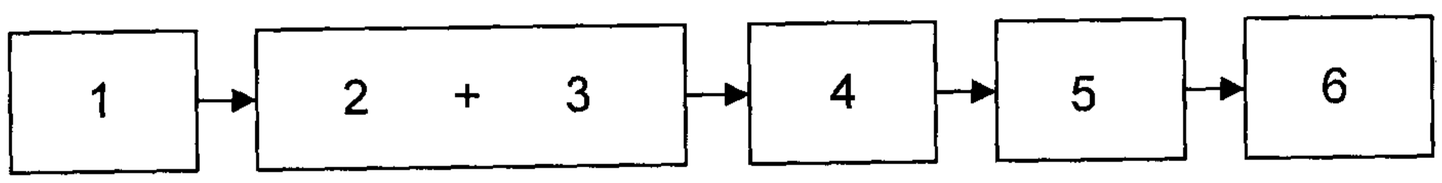


Figure 3

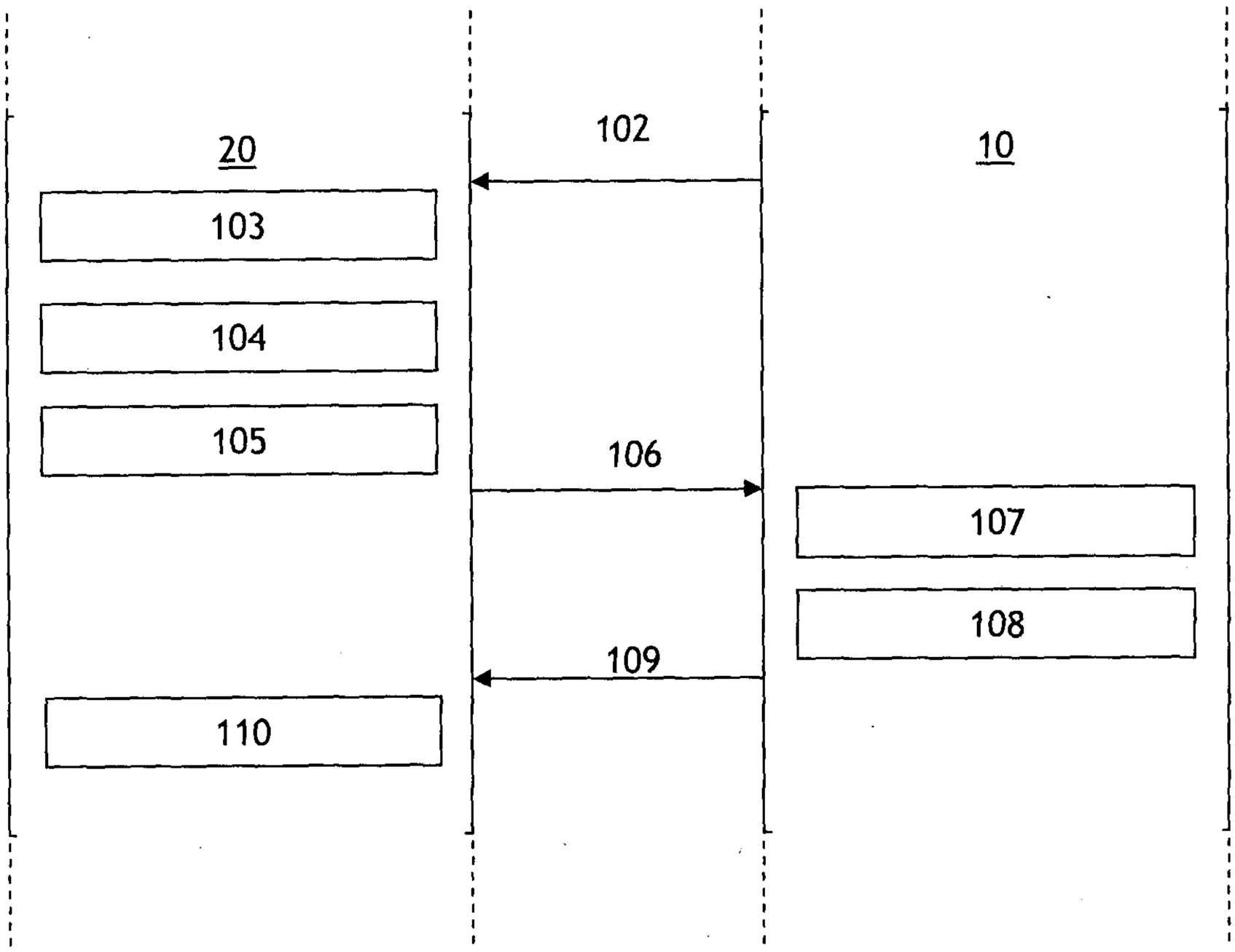


Figure 4

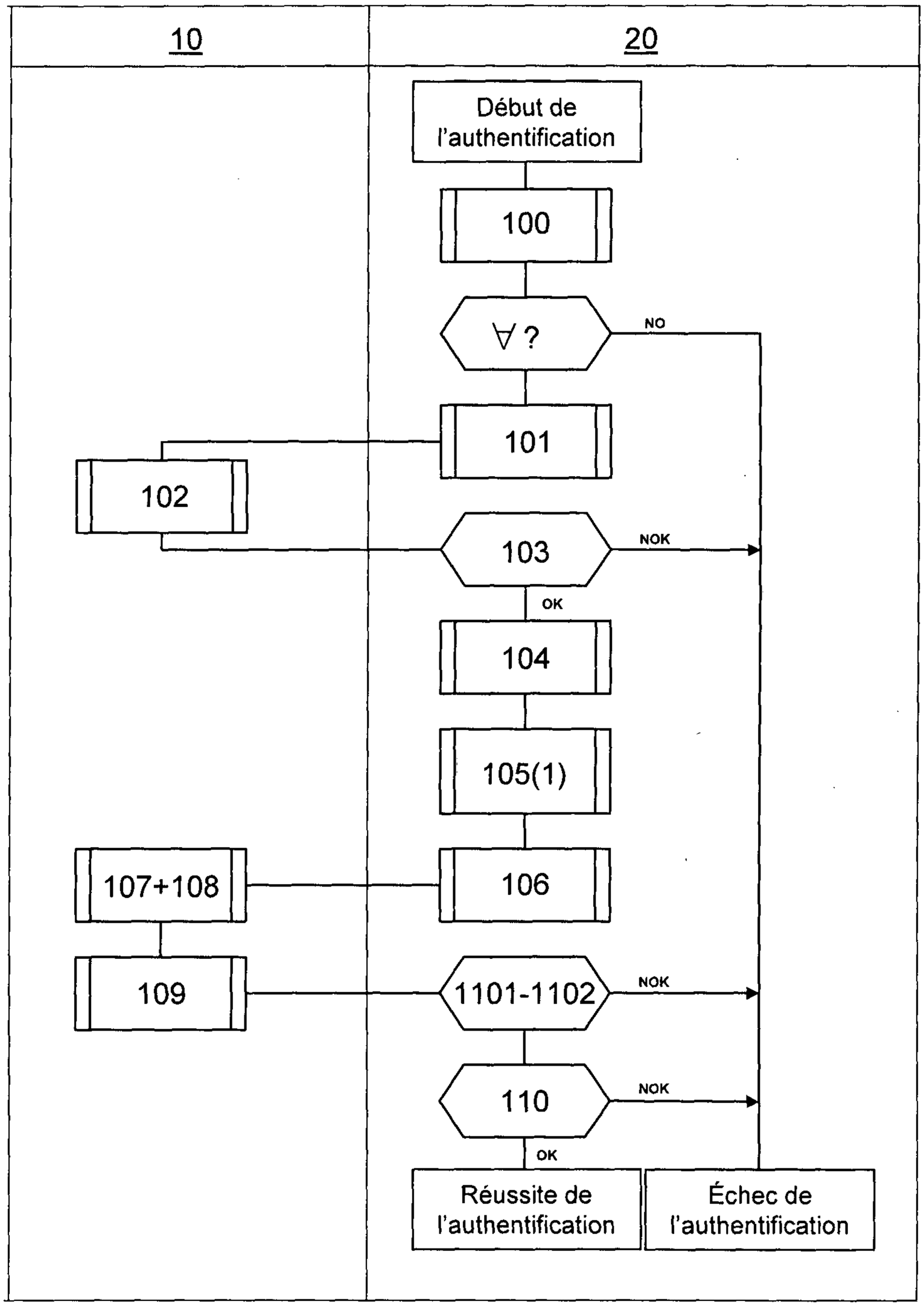

10
20
Début de l'authentification
100
∀ ?
NO
101
102
103
NOK
OK
104
105(1)
106
107+108
109
1101-1102
NOK
110
NOK
OK
Réussite de l'authentification
Échec de l'authentification

Figure 5

Code	Value				
CLA	'00'				
INS	'EE'				
P1	'00'				
P2	'00'				
Lc	Longueur du champ de données de commande				
DATA	'DB' Identifiant associé à la méthode sélectionnée de génération d'un canal de communication sécurisé				
	'DD' Identifiant associé au type de certificat sélectionné				
	'DF0D'	S-MAC	'DF0C'	S-ENC	chiffré avec la clé publique WPD
	'DF0E'	S-MASTER			
Le	Non présent				

74

73

71

72

70

Figure 6

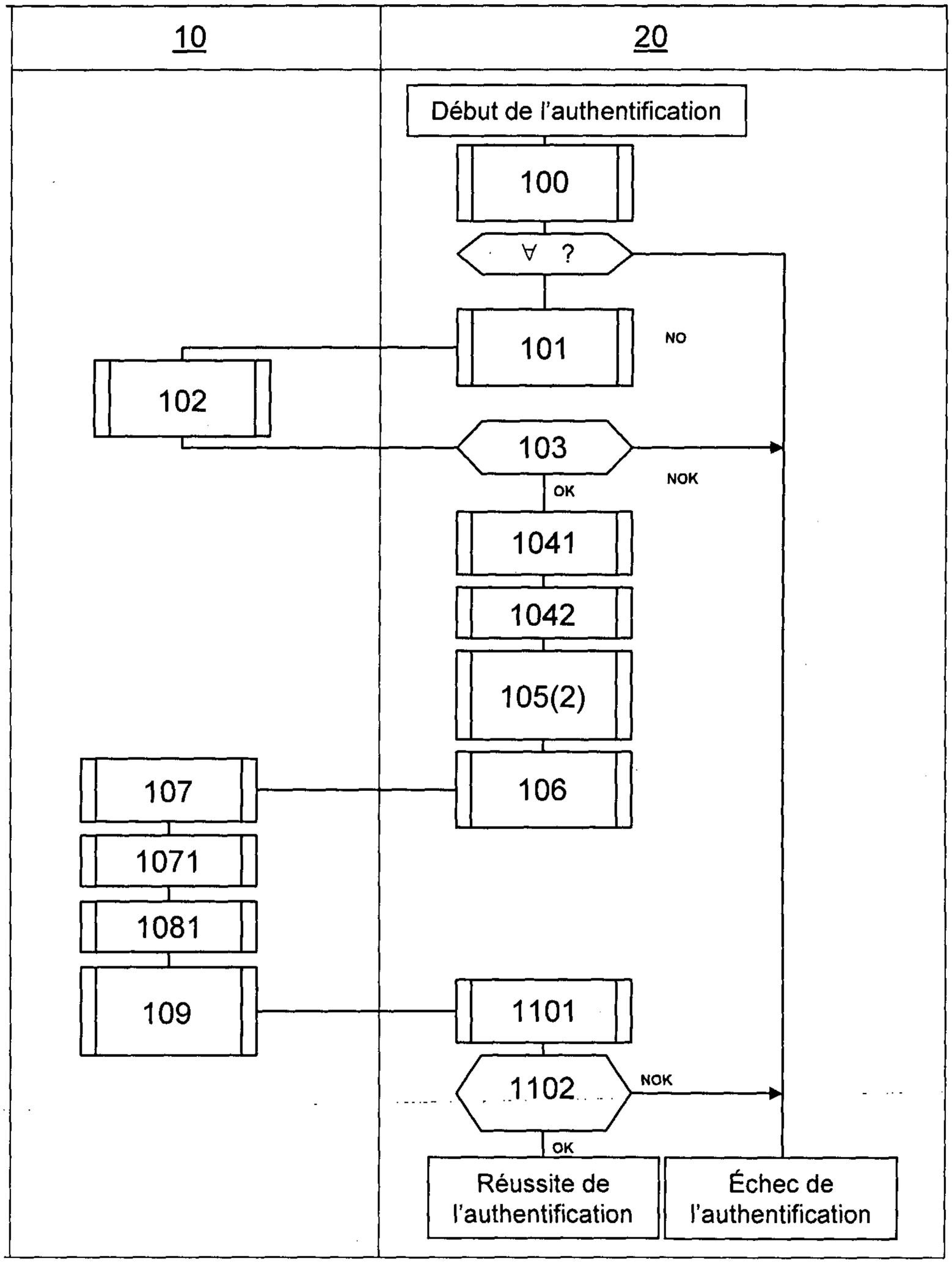

10
20
Début de l'authentification
100
∀ ?
101
NO
102
103
NOK
OK
1041
1042
105(2)
107
106
1071
1081
109
1101
1102
NOK
OK
Réussite de l'authentification
Échec de l'authentification

Figure 7

Code	Value	
CLA	'80'	
INS	'F0'	
P1	'C0	
P2	'20'	
Lc	Longueur du champ de données de commande (dépend de la longueur de la clé publique WPD)	
DATA	'DB' Identifiant associé à la méthode sélectionnée de génération d'un canal de communication sécurisé	
	'DD' Identifiant associé au type de certificat sélectionné	
	'DF18' Nombre aléatoire WAD	chiffré avec la clé publique WPD
	'DF17' Clé publique WAD	
Le	'00'	

82

80

81

Figure 8

Tag	Value	
'DF18'	Nombre aléatoire WAD	chiffré avec la clé publique WAD
'DF1B'	Nombre aléatoire WPD	

84

80

83

Figure 2