(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 810 822**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **00 08070**

(51) Int Cl[7] : **H 04 L 9/32,** G 06 K 9/00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 23.06.00.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 28.12.01 Bulletin 01/52.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

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

(71) **Demandeur(s) :** *FRANCE TELECOM Société anonyme* — FR.

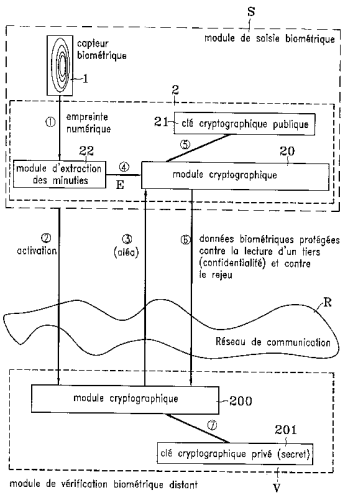
(72) **Inventeur(s) :** GUERIN DIDIER et GIRAULT MARC.

(73) **Titulaire(s) :**

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

(54) PROCEDE D'AUTHENTIFICATION/IDENTIFICATION BIOMETRIQUE SECURISE, MODULE DE SAISIE ET MODULE DE VERIFICATION DE DONNEES BIOMETRIQUES PERMETTANT DE METTRE EN OEUVRE LE PROCEDE.

(57) Procédé d'authentification biométrique sécurisé, comprenant la communication de données biométriques chiffrées à un module de vérification. Selon l'invention il est prévu de chiffrer les données biométriques par un algorithme cryptographique et d'introduire pour chaque opération cryptographique réalisée une valeur de diversification différente.



FR 2 810 822 - A1

PROCEDE D'AUTHENTIFICATION/IDENTIFICATION BIOMETRIQUE SECURISE, MODULE DE SAISIE ET MODULE DE VERIFICATION DE DONNEES BIOMETRIQUES PERMETTANT DE METTRE EN ŒUVRE LE PROCEDE.

La présente invention concerne un procédé d'authentification/identification de données biométriques sécurisés.

On parlera dans la suite de procédé d'authentification pour simplifier.

L'invention concerne également un module de saisie de données biométriques et un module de vérification desdites données permettant de mettre en œuvre le procédé, la coopération de ces modules entrant dans la réalisation d'un système d'authentification.

L'invention s'applique tout particulièrement au domaine de l'authentification ou de l'identification biométrique avec vérification par un dispositif placé à distance au travers d'un réseau de communication.

Par module de saisie de données biométriques on entend tout dispositif tel qu'un capteur biométrique permettant de relever les éléments biométriques d'un utilisateur du système d'authentification.

Par module de vérification de données biométriques on entend tout dispositif capable de traiter des informations biométriques pour les vérifier et vérifier leur authenticité. Il peut s'agir d'un ordinateur informatique ou d'une carte électronique spécifique placée dans un système de traitement.

On connaît du brevet publié le 23 juillet 1998 sous le numéro WO98/32093 un procédé de lutte contre le rejeu des données biométriques.

Par rejeu, on entend toute action malveillante consistant à capter les données biométriques d'un utilisateur du système d'authentification pour les envoyer au dispositif de vérification et se faire ainsi passer pour cet utilisateur.

Le procédé décrit dans cette demande repose sur le fait que les éléments biométriques caractéristiques également appelés « minuties » n'ont jamais la même valeur entre deux saisies. Le procédé décrit trouve une limitation dans le fait qu'il faut stocker les « minuties » reçues des précédents essais d'authentification et d'identification et dans le fait qu'il ne permet pas de se prémunir de données rejouées après avoir été légèrement modifiées de façon volontaire afin de tromper le système.

Il existe également des systèmes permettant la mise en œuvre d'un procédé biométrique avec vérification à distance des minuties et donc l'envoi de données au travers d'un réseau de communication.

Dans ce cas, soit les solutions proposées ne prennent pas en compte les problèmes liés au vol et au rejeu de données, soit elles associent des secrets cryptographiques dans les différents modules du système. On pourra trouver une telle solution par exemple dans la demande de brevet publiée le 06 novembre 1998 sous le numéro WO/9825385. En effet, le procédé décrit dans ce brevet protège les données contre une écoute sur la ligne mais ne permet pas de lutter contre le rejeu de données. Les deux modules en communication disposent d'un couple de clés privées publiques propres.

Dans le cas de secrets présents dans les différents modules du système, on peut craindre le vol du ou des secret(s) stocké(s) dans ces différents modules. Le vol

du ou des secret(s) stocké(s) dans les différents modules peut occasionner le vol des modules eux-mêmes et tout particulièrement du module de saisie biométrique qui est placé auprès du public.

Toutefois dans certaines solutions existantes les modules et notamment le module de saisie biométrique, peuvent ne pas mémoriser de secret en interne mais il est nécessaire alors que le secret soit apporté par l'utilisateur, au moyen par exemple d'une carte à puce ou d'un badge.

De tels systèmes sont décrits par exemple dans la demande de brevet publiée le 24 mars 1999 sous le numéro GB 2329499 ou dans la demande de brevet publiée le 27 janvier 1998 sous le numéro WO/9705578.

Avec cette dernière solution, la simplicité d'utilisation et l'ergonomie de la biométrie s'estompent puisque l'utilisateur est porteur d'un outil physique (une carte à puce ou un badge).

La présente invention a pour but de remédier à ces inconvénients.

L'invention permet en effet de fournir un procédé d'authentification ou d'identification biométrique organisé autour de modules de saisie biométriques raccordés, au moyen d'un réseau de communication non nécessairement sécurisé, à un ou plusieurs modules de vérification biométriques, tout en évitant les attaques par rejeu de données sans contraindre l'utilisateur au port d'un objet physique (carte à puce) et sans nécessiter la présence d'un ou de plusieurs secrets dans le ou les module(s) de saisie biométriques.

Ainsi, l'invention propose un procédé biométrique sécurisé comprenant un élément de sécurité contre le rejeu de données et un élément cryptographique assurant la confidentialité des données, aucun de ces éléments

ne requérant la présence d'un secret à l'endroit où les caractéristiques biométriques sont saisies, lesdites données incluant des données biométriques telles que des minuties.

La sécurité s'applique entre un module biométrique local, dénommé module de saisie biométrique et un module distant, dénommé module de vérification biométrique.

La mise en œuvre du procédé est transparente pour l'utilisateur souhaitant être authentifié. Ce dernier ne nécessite le port d'aucun outil physique destiné à la mise en œuvre du procédé. Il ne nécessite pas non plus que le module de vérification biométrique mémorise des valeurs à chaque authentification.

Le procédé proposé permet en particulier d'effectuer cette authentification à partir de modules biométriques distants du module de vérification et reliés par exemple à travers un réseau de communication ne nécessitant pas de sécurité particulière.

Le procédé d'authentification proposé permet de ne pas avoir à stocker un secret dans le module de saisie biométrique. Il permet également de garantir le non rejeu d'un envoi de données biométriques.

L'invention s'applique aux systèmes biométriques en général.

La présente invention a donc plus particulièrement pour objet un procédé d'authentification biométrique sécurisé, comprenant la communication de données biométriques chiffrées à un module de vérification, principalement caractérisé en ce qu'il consiste à chiffrer les données biométriques par un algorithme cryptographique et en ce qu'il consiste à introduire pour chaque opération cryptographique réalisée une valeur de diversification différente.

Selon un mode de réalisation, la valeur de diversification est générée par le module de vérification et communiquée au module de saisie des données biométriques.

Selon un autre mode de réalisation, la valeur de diversification est générée par le module de saisie et par le module de vérification.

La valeur de diversification est associée à la donnée biométrique, l'opération de chiffrement étant effectuée sur la donnée obtenue par cette association.

Selon une variante, la valeur de diversification est une donnée aléatoire.

Selon une autre variante, la valeur de diversification est le résultat d'un comptage.

Selon une autre variante, la valeur de diversification est une donnée temporelle (date, heure).

Selon un mode de réalisation l'algorithme de chiffrement est un algorithme asymétrique à clé publique.

Selon une variante la clé publique du module de vérification est communiquée au(x) module(s) de saisie par le module de vérification à chaque demande d'authentification.

Selon une autre variante la clé publique est stockée dans le module de saisie de données biométriques.

Selon une autre variante, la clé stockée dans le module de saisie est une clé de vérification d'un certificat, ledit certificat étant le certificat de la clé publique du module de vérification et étant communiqué par ce dernier au module de saisie.

Selon un autre mode de réalisation, l'algorithme de chiffrement est un algorithme symétrique à clé secrète.

Avantageusement, la clé secrète est générée par le module de saisie.

Avantageusement, la clé secrète est chiffrée par un algorithme asymétrique et le résultat du chiffrement est communiqué au module vérifieur pour lui permettre de déchiffrer les données biométriques.

L'invention a également pour objet, un module de saisie de données biométriques, principalement caractérisé en ce qu'il comporte des moyens pour effectuer des opérations de cryptographie pour chiffrer des données biométriques et introduire une valeur de diversification différente pour chaque opération selon l'une quelconque des revendications précédentes.

Selon une autre caractéristique, la valeur de diversification est générée par le module lui-même ou fournie par l'extérieur.

L'invention a aussi pour objet, un module de vérification de données biométriques, principalement caractérisé en ce qu'il comporte des moyens pour effectuer des opérations de cryptographie pour déchiffrer des données biométriques chiffrées reçues à travers un réseau de communication et contenant une valeur de diversification différente pour chaque donnée biométrique chiffrée.

Avantageusement, le module de vérification de données biométriques peut être relié par le réseau de communication à une pluralité de modules de saisie de données biométriques.

Selon une autre caractéristique, la valeur de diversification est générée par le module de vérification lui-même.

Les modules de saisie de données biométriques et le module de vérification peuvent être reliés par un réseau de communication non sécurisé.

D'autres particularités et avantages de l'invention apparaîtront clairement à la lecture de la description qui est faite ci-après et qui est donnée à titre illustratif et non limitatif en regard des dessins annexés sur lesquels :

- La figure 1, illustre de façon schématique la mise en œuvre d'un procédé d'authentification sécurisé selon l'invention,
- la figure 2, illustre un schéma d'implémentation pour la mise en œuvre du procédé dans un module de saisie biométrique et dans un module de vérification biométrique distant,
- la figure 3, illustre un système d'authentification de données biométriques selon l'invention,
- la figure 4, représente une variante du système d'authentification mettant en œuvre le procédé selon l'invention.

On va se reporter maintenant pour la suite de la description au schéma de la figure 1 dans sa partie I et dans sa partie II illustrant respectivement une première et une deuxième activation du procédé d'authentification biométrique.

La réalisation qui est donnée à titre d'exemple utilise comme protocole de cryptographie un algorithme à clé publique tel que l'algorithme RSA (Rivest Shamir Adleman).

L'algorithme RSA n'est pas le seul protocole pouvant convenir à la mise en œuvre de l'invention. Tous les protocoles d'échange de clé comme ceux décrits dans la norme ISO/IEC DIS 11770-3 Informations Technology Security Techniques Key Management-part 3 : *Mechanism Using Asymmetric Techniques*, conviennent dans

la mesure où le mécanisme utilisé permet l'authentification de l'entité en charge de vérifier l'identification/l'authentification biométrique et dans la mesure où cette entité est celle qui émet l'élément de diversification comme cela va être décrit dans la suite.

Le module de saisie biométrique S utilise une valeur dite de diversification VD pour protéger la communication des éléments biométriques de l'utilisateur contre le rejeu. Cette valeur peut être une valeur aléatoire, le résultat d'un compteur, un élément de temps, etc..

Le processus biométrique est activé dès lors qu'un utilisateur active le module de saisie S en se présentant devant le capteur biométrique 1.

L'activation provoque la génération d'une valeur de diversification VD.

Dans un premier mode de réalisation d'implémentation du procédé illustré par cette figure 1, la génération de la valeur de diversification est faite par le module de vérification V.

C'est pourquoi l'activation du procédé se traduit pour ce mode de réalisation, par une demande de valeur de diversification VD du module de saisie S au module de vérification V (action A sur le dessin).

Le module de vérification biométrique V fournit alors une valeur de diversification au module de saisie biométrique S (action B). Le module de saisie biométrique S extrait les éléments caractéristiques E de l'élément biométrique, y associe l'élément de diversification VD et effectue une opération de chiffrement C portant principalement sur ces paramètres, sous le contrôle de la fonction

cryptographique asymétrique publique e_v et envoie le résultat C au module de vérification (action C)..

L'opération de chiffrement se traduit par la relation suivante :

$C = e_v (E+VD)$.

(le signe + symbolisant une caractérisation des données.)

Le calcul cryptographique permet de garantir que seul le possesseur de la clé privée appropriée sera en mesure d'interpréter correctement les données biométriques envoyées et de vérifier que l'élément de diversification a été pris en compte et ceci en vérifiant que :

dv(C) est égale à (E+VD) ; dv étant la fonction de déchiffrement.

Le rejeu est évité car si une nouvelle procédure d'authentification est mise en œuvre pour une même personne, c'est-à-dire une personne qui aurait une même donnée biométrique E, la valeur de diversification qui est générée (et envoyée par le système de vérification) ne sera pas la même et sera égale à une valeur VD' comme l'illustre la partie II du schéma de la figure 1. Autrement dit une personne mal intentionnée qui aurait pendant l'étape I réussi à obtenir l'information C sur la ligne et rejouerait cette information C de chiffrement, aboutirait à un échec au moment de la vérification car la valeur de diversification n'est plus VD mais une nouvelle valeur VD'.

Selon le mode de réalisation qui vient d'être décrit, l'élément de diversification VD est généré par le module de vérification biométrique et envoyé au module de saisie biométrique (action A).

Selon un autre mode de réalisation, il peut être envisagé que la valeur de diversification soit générée

par le module de saisie biométrique lui-même. Dans ce cas, le module de vérification biométrique devra être en mesure de générer lui aussi cette valeur de diversification. On comprend que dans ce cas il ne s'agira pas d'une valeur aléatoire mais d'une date par exemple. Ainsi, le module de vérification sera en mesure de vérifier que les données envoyées ne sont pas le rejeu d'un envoi précédent.(L'action A disparaît dans ce mode de réalisation).

Selon ce mode de réalisation le module de saisie biométrique comporte en mémoire la clé publique de l'algorithme de cryptographie asymétrique à clé publique, pour effectuer le calcul cryptographique sous le contrôle de la clé cryptographique asymétrique publique du module de vérification biométrique. Ce calcul cryptographique permet comme on l'a dit de garantir que seul le module de vérification biométrique, possesseur de la clé privée appropriée d_v sera en mesure d'interpréter correctement les données biométriques envoyées et de vérifier que la valeur de diversification a été prise en compte.

Selon un autre mode de réalisation il peut être envisagé que la clé stockée en permanence dans une mémoire du module de saisie biométrique soit une clé de vérification de certificat. Dans ce cas le module de vérification biométrique V envoie au module de saisie biométrique un élément de diversification VD et sa clé publique de chiffrement certifiée $Cert(PUBe_v)$. Le certificat est vérifié avec la clé contenue en permanence dans la mémoire du module de saisie biométrique. Après vérification positive du certificat, le module de saisie biométrique utilise la clé publique du module de vérification biométrique pour assurer la confidentialité des données biométriques qu'il va

ensuite transmettre au module de vérification biométrique.

Selon un autre mode de réalisation il peut être envisagé que le module de saisie génère une clé secrète cl pour chiffrer les données à transmettre au moyen d'un algorithme symétrique utilisant cette cl. Typiquement l'algorithme utilisé pourra être un algorithme triple DES (Data Encryption Standard). Le module de saisie chiffre alors les données concaténées E+VD au moyen de cet algorithme symétrique et de la clé secrète cl générée à cette fin et transmet les données ainsi chiffrées au module de vérification. Comme le module de vérification ne possède pas la clé secrète générée par le module de saisie, ce dernier envoie la clé secrète chiffrée par l'algorithme à clé publique pour lui permettre de déchiffrer les données reçues. Le module de vérification réalise la fonction inverse correspondant à l'algorithme de chiffrement pour obtenir la valeur déchiffrée E+VD.

Il peut être prévu en outre que la clé privée cl soit concaténée à un aléa et de chiffrer la donnée ainsi obtenue au moyen de l'algorithme à clé publique.

On va maintenant se reporter au schéma de la figure 2. Ce schéma illustre l'implémentation du procédé selon l'invention dans un module de saisie biométrique S et dans un module de vérification biométrique distant V. Le module de saisie biométrique comporte de manière connue en soi un capteur biométrique 1. Ce capteur fournit une empreinte numérique d'un utilisateur du système à un module d'extraction de minuties 22 apte à envoyer les éléments E issus de cette extraction au module cryptographique 20 résidant dans le module de saisie biométrique S. Le module de cryptographie est réalisé par exemple par un cryptoprocesseur du commerce

associé à une mémoire non volatile 21 comprenant la clé publique, à savoir les paramètres $PUBe_v$, (si $PUBe_v$ est le nom de cette clé).

Comme on peut le suivre à partir de la numérotation 1 à 7 apparaissant sur ce schéma, lorsqu'un opérateur désire effectuer une opération d'authentification il se présente devant le capteur biométrique 1 qui réalise une empreinte numérique d'une donnée biométrique de l'utilisateur. Le capteur transmet cette empreinte au module d'extraction des minuties 22. Le module d'extraction transmet au module cryptographique les données issues de cette extraction et le module cryptographique réalise l'opération de chiffrement sur ces données à partir des paramètres de l'algorithme de cryptographie et après avoir reçu du module de vérification biométrique distant la donnée de diversification VD. Le module de vérification biométrique est activé dès l'activation du capteur biométrique 1.

Le module de vérification V comporte également un module cryptographique 200 associé à une mémoire non volatile 201 qui stocke la clé privée, c'est-à-dire le secret utilisé dans l'algorithme de cryptographie à clé publique, à savoir le paramètre $PRIVd_v$ (si $PRIVd_v$ est le nom de la clé privée)

Conformément à l'invention et tous ces modes de réalisation, il n'y a pas de stockage de secret dans le module de saisie biométrique. Ce module de saisie biométrique est un module qui peut être implanté dans des bâtiments publics et relié à travers un réseau de communication R à un module de vérification biométrique V, qui lui va détenir le secret.

Le schéma de la figure 3 illustre un système d'authentification mettant en œuvre le procédé conforme à l'invention.

Comme on peut le voir sur le schéma de la figure 4, le procédé conforme à l'invention est tout à fait adapté à une implantation d'un système d'authentification dans laquelle plusieurs modules de saisie biométriques S indépendants et distants peuvent être reliés à travers un réseau de communication à un seul et même module de vérification biométrique V.

Ainsi, la présente invention permet d'implémenter un procédé d'identification/authentification biométrique sans que les vérifications biométriques soient effectuées en local (par rapport au module de saisie biométrique et à l'utilisateur), sans craindre le vol et le rejeu de données biométriques et sans placer d'éléments cryptographiques secrets dans le module de saisie biométrique.

Il peut par exemple être envisagé un mécanisme de contrôle d'accès biométrique équipé de plusieurs modules de saisie biométrique reliés à un seul module de vérification biométrique centralisé, comme l'illustre la figure 4.

Pour illustration il peut être envisagé un service de contrôle d'accès appliqué à l'ouverture-fermeture d'un accès physique (portes d'immeubles, etc.) ou d'un accès logique (serveur informatique, etc.).

REVENDICATIONS

1. Procédé d'authentification biométrique sécurisé, comprenant la communication de données biométriques chiffrées à un module de vérification, caractérisé en ce qu'il consiste à chiffrer les données biométriques par un algorithme cryptographique et en ce qu'il consiste à introduire pour chaque opération cryptographique réalisée une valeur de diversification différente.

2. Procédé d'authentification biométrique sécurisé selon la revendication 1, caractérisé en que la valeur de diversification est générée par le module de vérification et communiquée au module de saisie des données biométriques.

3. Procédé d'authentification biométrique sécurisé selon la revendication 1, caractérisé en que la valeur de diversification est générée par le module de saisie et par le module de vérification.

4. Procédé d'authentification biométrique sécurisé selon l'une quelconque des revendications précédentes, caractérisé en que la valeur de diversification est associée à la donnée biométrique, l'opération de chiffrement étant effectuée sur la donnée obtenue par cette association.

5. Procédé d'authentification biométrique sécurisé selon l'une quelconque des revendications précédentes, caractérisé en que la valeur de diversification est une donnée aléatoire.

6. Procédé d'authentification biométrique sécurisé selon les revendications 1 à 4, caractérisé en que la valeur de diversification est le résultat d'un comptage.

7. Procédé d'authentification biométrique sécurisé selon les revendications 1 à 4, caractérisé en que la valeur de diversification est une donnée temporelle (date, heure).

8. Procédé d'authentification biométrique sécurisé selon les revendications 1 à 4, caractérisé en que l'algorithme de chiffrement est un algorithme asymétrique à clé publique.

9. Procédé d'authentification biométrique, selon la revendication 8, caractérisé en ce que la clé publique du module de vérification est communiquée au(x) module(s) de saisie par ledit module de vérification à chaque demande d'authentification.

10. Procédé d'authentification biométrique sécurisé selon la revendication 8, caractérisé en que la clé publique est stockée dans le module de saisie de données biométriques.

11. Procédé d'authentification biométrique sécurisé selon la revendication 10, caractérisé en que la clé stockée dans le module de saisie est une clé de vérification d'un certificat, ledit certificat étant le certificat de la clé publique du module de vérification et étant communiqué par ce dernier au module de saisie.

12. Procédé d'authentification biométrique selon l'une quelconque des revendications 1 à 7, caractérisé en ce que l'algorithme de chiffrement est un algorithme symétrique à clé secrète.

13.Procédé d'authentification biométrique selon la revendication 12, caractérisé en ce que la clé secrète est générée par le module de saisie.

14.Procédé d'authentification biométrique selon la revendication 13, caractérisé en ce que la clé secrète est chiffrée par un algorithme asymétrique et le résultat du chiffrement est communiqué au module de vérification pour lui permettre de déchiffrer les données biométriques.

15. Module de saisie de données biométriques, caractérisé en ce qu'il comporte des moyens pour effectuer des opérations de cryptographie pour chiffrer des données biométriques et introduire une valeur de diversification différente pour chaque opération selon l'une quelconque des revendications précédentes.

16. Module de saisie de données biométriques, selon la revendication 15, caractérisé en ce que la valeur de diversification est générée par le module lui-même ou fournie par l'extérieur.

17. Module de vérification de données biométriques, caractérisé en ce qu'il comporte des moyens pour effectuer des opérations de cryptographie pour déchiffrer des données biométriques chiffrées reçues à travers un réseau de communication et contenant une valeur de diversification différente pour chaque donnée

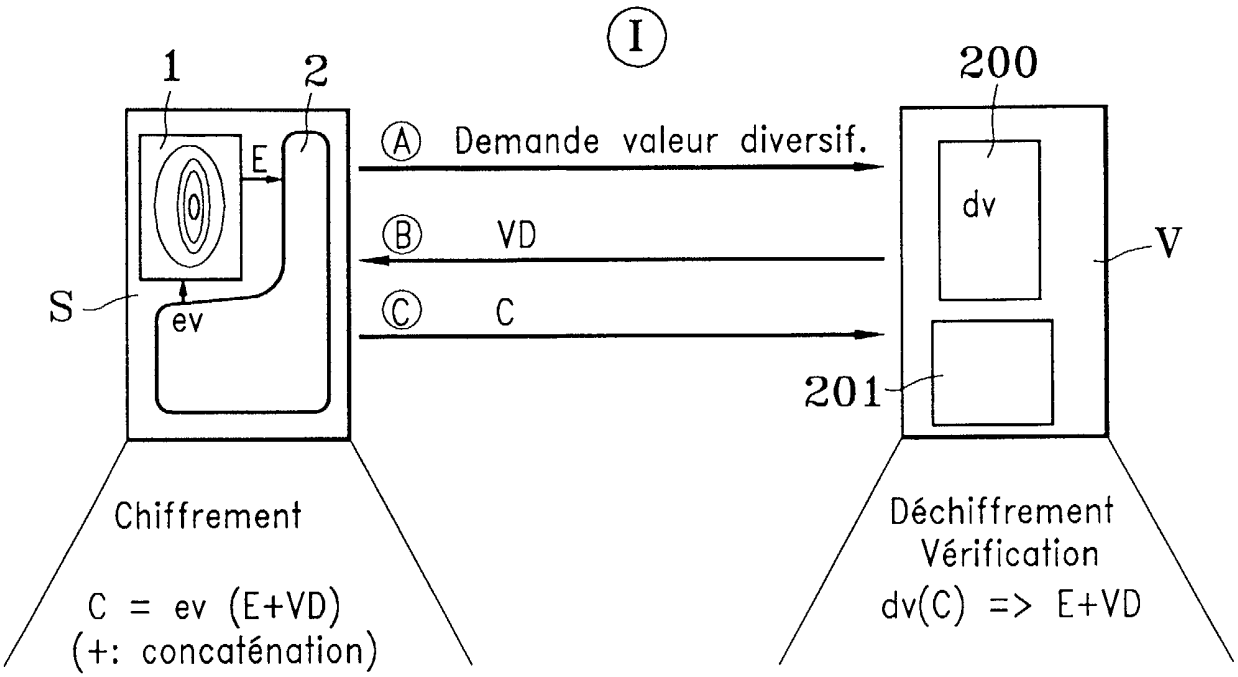
biométrique chiffrée selon l'une quelconque des revendications 1 à 15.

18. Module de vérification de données biométriques selon la revendication 17, caractérisé en ce qu'il est relié par le réseau de communication à une pluralité de modules de saisie de données biométriques.

19. Module de vérification de données biométriques, selon la revendication 17 ou 18, caractérisé en ce que la valeur de diversification est générée par le module de vérification lui-même.

20. Module de vérification de données biométriques selon l'une quelconque des revendications 15 à 19, caractérisé en ce que les modules de saisie de données biométriques et le module de vérification sont reliés par un réseau de communication non sécurisé.

FIG. 1


I
1
2
200
E
Ⓐ Demande valeur diversif.
dv
Ⓑ VD
V
S
ev
Ⓒ C
201
Chiffrement
C = ev (E+VD)
(+: concaténation)
Déchiffrement
Vérification
dv(C) => E+VD

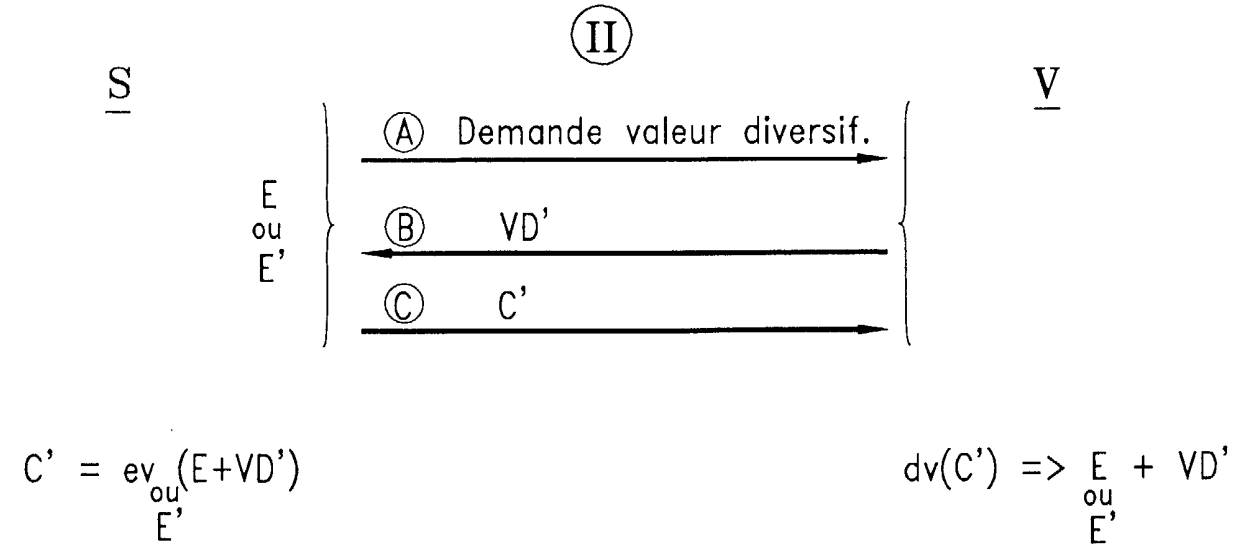

II
S
V
Ⓐ Demande valeur diversif.
E
ou
E'
Ⓑ VD'
Ⓒ C'
C' = ev ou E' (E+VD')
dv(C') => E ou E' + VD'

FIG.2

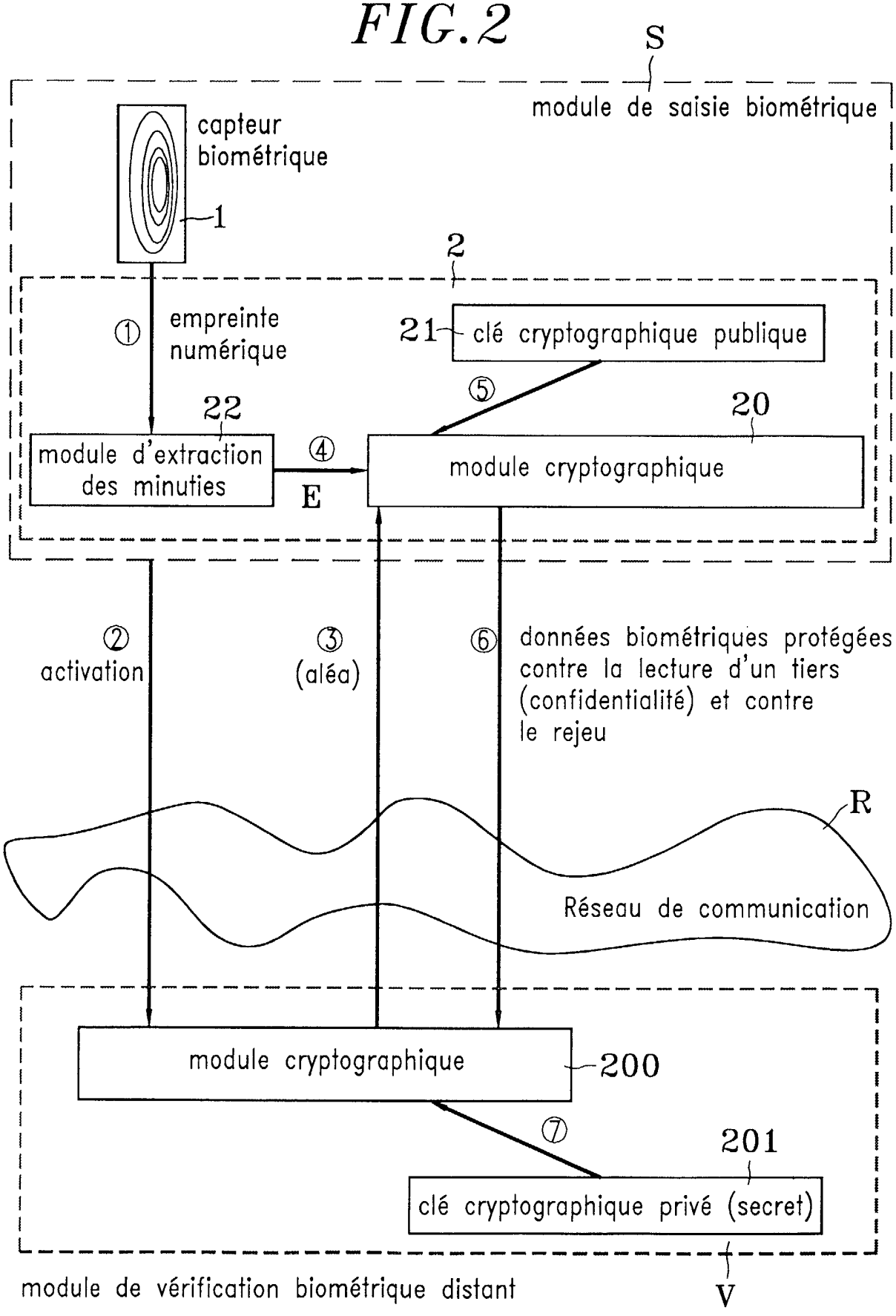

S
module de saisie biométrique
capteur biométrique
1
2
① empreinte numérique
21 clé cryptographique publique
⑤
22
20
module d'extraction des minuties
④
E
module cryptographique
② activation
③ (aléa)
⑥ données biométriques protégées contre la lecture d'un tiers (confidentialité) et contre le rejeu
R
Réseau de communication
module cryptographique
200
⑦
201
clé cryptographique privé (secret)
module de vérification biométrique distant
V

FIG.3

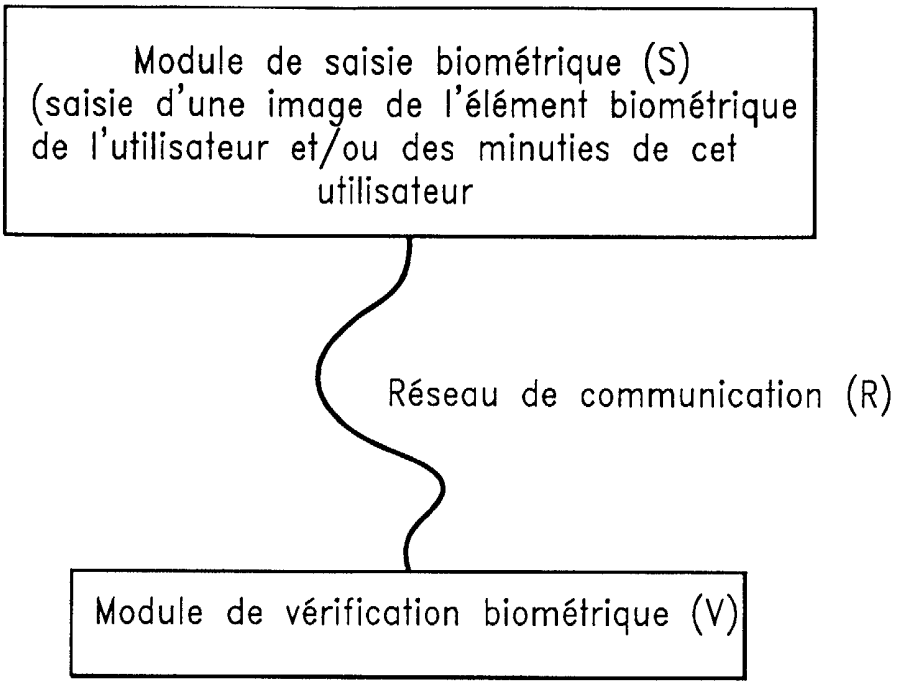
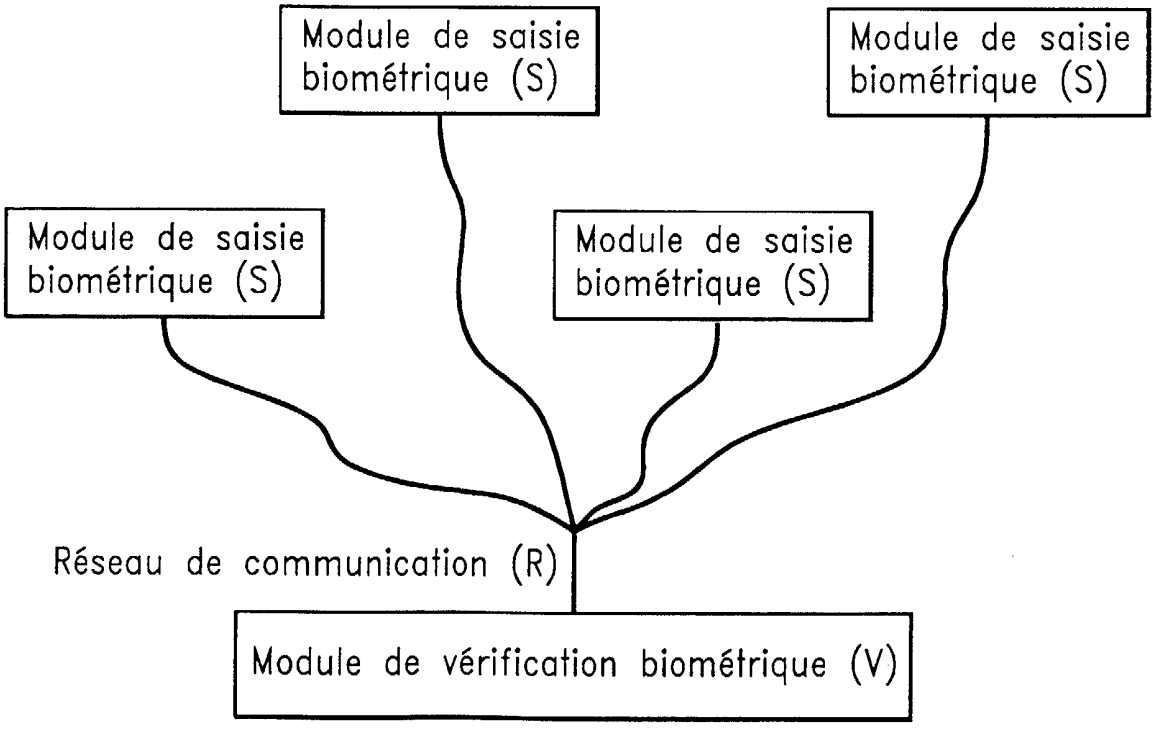

Module de saisie biométrique (S)
(saisie d'une image de l'élément biométrique de l'utilisateur et/ou des minuties de cet utilisateur
Réseau de communication (R)
Module de vérification biométrique (V)

FIG.4


Module de saisie biométrique (S)
Module de saisie biométrique (S)
Module de saisie biométrique (S)
Module de saisie biométrique (S)
Réseau de communication (R)
Module de vérification biométrique (V)

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2810822

N° d'enregistrement national

FA 588902
FR 0008070

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	WO 00 00882 A (LCI SMARTPEN NV) 6 janvier 2000 (2000-01-06) * page 4, ligne 19 - ligne 25 * * page 6, ligne 7 - ligne 11 * * page 11, ligne 16 - page 12, ligne 4 * * page 12, ligne 12 - ligne 16 * ---	1,6,8, 12,15,16	H04L9/32 G06K9/00
D,Y	WO 98 25385 A (BORZA STEPHEN J ;DEW ENGINEERING AND DEV LIMITE (CA)) 11 juin 1998 (1998-06-11) * page 12, ligne 1 - ligne 18 * ---	1,6-8,15	
Y	US 5 351 295 A (PERLMAN RADIA J ET AL) 27 septembre 1994 (1994-09-27) * colonne 2, ligne 49 - ligne 58 * * colonne 4, ligne 32 - ligne 51 * -----	1,6-8,15	
			DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7) H04L G06F

Date d'achèvement de la recherche	Examinateur
23 mars 2001	Holper, G

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

.....

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)