(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 2 871 615 A1**

(12) **DEMANDE DE BREVET EUROPEEN**

(43) Date de publication:
13.05.2015 Bulletin 2015/20

(51) Int Cl.:
G07C 9/00 *(2006.01)*

(21) Numéro de dépôt: **13192404.5**

(22) Date de dépôt: **12.11.2013**

(84) Etats contractants désignés:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Etats d'extension désignés:
BA ME

(71) Demandeur: **Nagravision S.A.**
1033 Cheseaux-sur-Lausanne (CH)

(72) Inventeur: **Bocchetti, Salvatore**
1004 Lausanne (CH)

(74) Mandataire: **Leman Consulting S.A.**
Chemin de Précossy 31
1260 Nyon (CH)

(54) **Méthode d'authentification d'un utilisateur par un module d'authentification**

(57) La présente invention concerne une méthode d'authentification d'un utilisateur par un module d'authentification, ledit module d'authentification gérant l'accès à une pluralité de services et comprenant un seuil d'authentification pour chaque service, au moins deux données d'authentification étant associées audit utilisateur, ladite méthode comprenant les étapes d'acquisition d'au moins une donnée d'authentification de l'utilisateur, au moyen d'une interface entre cet utilisateur et ledit module d'authentification; et de vérification de ladite au moins une donnée d'authentification et attribution d'une valeur d'authentification à l'utilisateur, en fonction du résultat de la vérification; de comparaison de la valeur d'authentification avec la valeur de seuil pour le service requis. Si la valeur d'authentification est égale ou supérieure à la valeur de seuil, l'accès au service requis par l'utilisateur est autorisé. Si la valeur d'authentification est inférieure à la valeur de seuil, vérification si une donnée d'authentification non utilisée est disponible pour cet utilisateur; si aucune donnée d'authentification non utilisée n'est disponible pour cet utilisateur, refus de l'accès au service requis. Si au moins une donnée d'authentification non utilisée est disponible pour cet utilisateur, la méthode est répétée en acquérrant une donnée d'authentification différente de celle(s) présentée(s) antérieurement et en combinant les valeurs d'authentification, la comparaison étant faite entre la valeur de seuil et la combinaison des valeurs d'authentification.

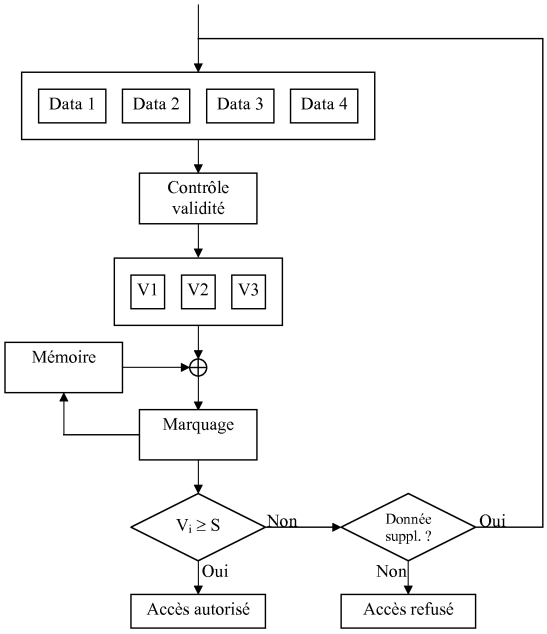

Fig. 1

EP 2 871 615 A1

Description

DOMAINE TECHNIQUE

[0001] La présente invention concerne une méthode d'authentification d'un utilisateur par un module d'authentification gérant l'accès à une pluralité de services.

TECHNIQUE ANTERIEURE

[0002] L'authentification d'un utilisateur est un problème complexe qui doit prendre en compte plusieurs paramètres contradictoires tels qu'en particulier la sécurité et la facilité d'utilisation.

[0003] Les méthodes actuelles sont basées sur une ou plusieurs caractéristiques que l'utilisateur et le fournisseur de services ont dû convenir au préalable. Ces caractéristiques ou secrets, dénommés ci-après données d'authentification, sont mémorisées dans un module d'authentification associé au fournisseur de services. Les données d'authentification peuvent être classées en trois catégories. L'une des catégories contient quelque chose que l'utilisateur connaît (mot de passe, réponse à une question secrète, règle secrète,..). Une autre catégorie contient quelque chose que l'utilisateur possède (téléphone portable, carte à puce,...) et la dernière catégorie contient quelque chose que l'utilisateur est, c'est-à-dire essentiellement les données biométriques et les données liées au comportement habituel de l'utilisateur (empreinte digitale, conformation de l'oeil, manière de taper un mot de passe, ..).

[0004] Dans les systèmes d'authentification actuels, pour accéder à un service sécurisé proposé par un fournisseur de services ou accessible depuis un dispositif ou un appareil, une ou plusieurs données d'authentification sont demandées à l'utilisateur. Les réponses données par l'utilisateur sont transmises à un module d'authentification dans lequel elles sont comparées aux réponses attendues par ce module d'authentification. Si les réponses concordent, l'accès au service est autorisé.

[0005] Il arrive, dans certaines circonstances ou dans certains systèmes, que plusieurs données d'authentification soient demandées à l'utilisateur et qu'une réponse partielle ne soit pas suffisante pour accéder au service. Ceci peut être le cas lors de l'utilisation de certaines applications demandant un niveau de sécurité élevé où par exemple un mot de passe est demandé en plus d'informations biométriques. Cela peut également être le cas lorsque le module d'authentification détecte quelque chose d'inhabituel tel que par exemple une tentative de connexion à un serveur depuis une adresse IP inhabituelle. Dans ce cas, le module d'authentification peut, après avoir reçu un mot de passe correct, demander une confirmation en demandant par exemple la réponse à une question secrète ou une adresse e-mail de "secours", mémorisée lors d'une phase d'initialisation.

[0006] Dans tous les cas, le niveau de sécurité est fixé à l'avance et le système n'est pas flexible. De plus, l'accès à un service se fait de façon binaire, c'est-à-dire qu'une donnée est considérée soit comme juste, soit comme fausse. Par exemple, si le mot de passe introduit par l'utilisateur est faux, l'accès au service est interdit.

[0007] Les méthodes actuelles destinées à vérifier l'authenticité d'un utilisateur souhaitant accéder à un service sont donc peu flexibles en ce sens qu'elles ne permettent pas d'être adaptées au niveau de sécurité requis par le service et/ou à certains souhaits de l'utilisateur. Si le niveau de sécurité est trop élevé, la facilité d'utilisation risque d'être faible et la procédure d'authentification peut être contraignante ou même rédhibitoire pour l'utilisateur. Au contraire, si l'accès est simple pour l'utilisateur, la sécurité pourrait être trop faible.

[0008] Il est donc souhaitable d'avoir une méthode flexible, dans laquelle le niveau de sécurité peut être varié facilement, par exemple en fonction du service demandé ou en fonction de choix de l'utilisateur ou du fournisseur.

EXPOSE DE L'INVENTION

[0009] Le but de l'invention est atteint par une méthode d'authentification d'un utilisateur par un module d'authentification, ledit module d'authentification gérant l'accès à une pluralité de services et comprenant un seuil d'authentification pour chaque service, au moins deux données d'authentification étant associées audit utilisateur, ladite méthode comprenant les étapes suivantes :

a) acquisition d'au moins une donnée d'authentification de l'utilisateur, au moyen d'une interface entre cet utilisateur et ledit module d'authentification;

b) vérification de ladite au moins une donnée d'authentification et attribution d'une valeur d'authentification à l'utilisateur, en fonction du résultat de la vérification;

c) comparaison de la valeur d'authentification avec la valeur de seuil pour le service requis;

d) si la valeur d'authentification est égale ou supérieure à la valeur de seuil, accorder l'accès au service requis par l'utilisateur;

e) si la valeur d'authentification est inférieure à la valeur de seuil, vérification si une donnée d'authentification non utilisée est disponible pour cet utilisateur;

f) si aucune donnée d'authentification non utilisée n'est disponible pour cet utilisateur, refus de l'accès au service requis;

g) si au moins une donnée d'authentification non utilisée est disponible pour cet utilisateur, répétition des étapes a) à f) en acquérrant une donnée d'authen-

tification différente de celle(s) présentée(s) antérieurement et en combinant les valeurs d'authentification, ladite comparaison étant faite entre la valeur de seuil et la combinaison des valeurs d'authentification.

[0010] Selon la présente méthode, l'authentification d'un utilisateur souhaitant accéder à un service se fait de façon très souple. Le niveau de sécurité peut en particulier être adapté au service auquel l'utilisateur souhaite accéder et à d'autres conditions liées à l'environnement, telles que par exemple l'heure du jour. Un niveau de sécurité élevé peut être requis pour des services tels que des paiements ou tous services pour lesquels une usurpation d'identité peut avoir des conséquences importantes, alors qu'un niveau de sécurité plus bas peut être requis pour des services dans lesquels une usurpation d'identité a peu de conséquences.

[0011] Selon cette invention, l'utilisateur et le module d'authentification peuvent partager plusieurs secrets ou données d'authentification. Au moins l'une de ces données d'authentification est en principe introduite dans le module d'authentification lors d'une phase d'initialisation, par exemple à la conclusion d'un abonnement. Comme cela est expliqué en détail ci-dessous, il est possible qu'une seule donnée d'authentification ne soit pas suffisante pour accéder à tous les services proposés par un fournisseur. Il est possible d'introduire des secrets ou des données d'authentification supplémentaires en même temps que la première donnée d'authentification, ou par la suite, par exemple lorsque l'utilisateur souhaite pouvoir accéder à des services supplémentaires. Certaines données d'authentification peuvent être acquises sans la participation active et éclairée de l'utilisateur. Ainsi, le comportement de l'utilisateur peut être mémorisé sans que ce dernier en soit informé ou ne s'en rende compte, ce comportement formant un secret ou une donnée d'authentification utilisable dans le cadre de la présente invention.

[0012] Selon un mode de réalisation de l'invention, l'utilisateur peut choisir sur la base de quelle donnée d'authentification il souhaite accéder au service. A titre d'exemple, si un utilisateur peut accéder à un service au moyen d'une carte à puce, d'un mot de passe ou de données biométriques, il aura le choix du type de données et pourra accéder au service même s'il n'a pas la carte à puce à disposition, par exemple en choisissant d'utiliser les données biométriques.

[0013] Selon une variante, les données d'authentification à fournir au module d'authentification pourront varier en fonction du type de services requis. Un certain choix pourra toutefois être laissé à l'utilisateur. A titre d'exemple, l'accès à un service pour lequel l'usurpation d'identité aura peu de conséquences pourra être autorisé avec, au choix de l'utilisateur, une information parmi un mot de passe, une carte à puce ou une donné biométrique. L'accès à un service requérant un niveau de sécurité plus élevé pourra par exemple se faire seulement avec un mot de passe combiné avec une carte à puce ou le mot de passe combiné avec une donnée biométrique.

[0014] Selon une variante, le fournisseur de données peut suggérer ou imposer à l'utilisateur, les données d'authentification que celui-ci doit utiliser pour accéder au service requis. Dans cette variante, le fournisseur peut proposer d'utiliser un donnée d'authentification suffisante pour accéder au service requis, mais ayant la valeur la plus faible possible pour un tiers interceptant cette donnée. En effet, plus la valeur est élevée pour l'utilisateur, plus elle est également élevée pour un usurpateur. Il peut donc être intéressant d'utiliser les informations qui sont suffisantes pour accéder au service considéré, mais qui ont le moins de valeur possible pour un usurpateur.

[0015] La méthode de l'invention permet d'utiliser de façon efficace, des données d'authentification pour lesquelles la vérification de la conformité entre ce qui est reçu par le module d'authentification et ce qui est attendu peut être difficile à évaluer de façon binaire. Ceci peut être le cas par exemple en analysant le comportement de l'utilisateur lors de l'introduction d'un mot de passe ou d'une phrase secrète (passphrase). Un utilisateur donné aura généralement une manière d'écrire son mot de passe de façon reproductible. En particulier, le temps requis pour écrire le mot de passe, l'intervalle entre deux touches consécutives,.. seront très proches d'une fois à l'autre. Un autre utilisateur introduisant le même mot de passe aura très vraisemblablement un comportement différent. Ce type de données pourra être utilisé dans la méthode de l'invention.

[0016] Le niveau de sécurité minimal est en principe fixé par le fournisseur de services. Il est possible toutefois pour l'utilisateur de fixer un niveau de sécurité plus élevé que ce niveau minimal. Ceci peut être fait par chaque utilisateur, de façon individualisée. Cette augmentation du niveau de sécurité se fait généralement au détriment de la facilité d'utilisation. Chaque utilisateur pourra adapter le niveau de sécurité et la facilité d'utilisation selon ses désirs, dans le cadre fixé par le fournisseur de services. En règle générale, un utilisateur ne pourra toutefois pas fixer un niveau de sécurité en dessous du niveau de sécurité minimal fixé par le fournisseur de services pour le service considéré.

DESCRIPTION SOMMAIRE DES DESSINS

[0017] La présente invention et ses avantages seront mieux compris en référence aux figures annexées et à la description détaillée d'un mode de réalisation particulier, dans lesquelles :

- la figure 1 illustre sous forme de schéma bloc, le déroulement de la méthode de l'invention;
- la figure 2 représente de façon schématique, un exemple de réalisation de l'invention.

MANIERES DE REALISER L'INVENTION

[0018] La présente invention concerne une méthode pour authentifier un utilisateur qui souhaite accéder à un service. Cette authentification se fait au moyen d'un module d'authentification, en utilisant une interface entre l'utilisateur et le module d'authentification.

[0019] Cette interface peut être un clavier tel qu'un clavier alphanumérique au moyen duquel l'utilisateur peut introduire un code d'accès, un mot de passe, une phrase secrète, une valeur résultant d'un calcul, ... L'interface peut également comporter un capteur et un dispositif de traitement, le capteur pouvant être utilisé pour la détection d'informations biométriques telles que les empreintes digitales, la reconnaissance faciale, la reconnaissance rétinienne,... L'interface comporte généralement un affichage permettant à l'utilisateur de lire des instructions qui lui sont destinées.

[0020] L'utilisateur peut être amené à introduire des données de façon active (mot de passe, code PIN,...) ou laisser l'interface acquérir les données (empreintes digitales, reconnaissance rétinienne, reconnaissance vocale, ...)

[0021] Le procédé de l'invention peut être utilisé pour accéder à un service spécifique d'un fournisseur, ce fournisseur proposant un accès à un ou plusieurs services. Un tel fournisseur de services peut par exemple être une banque, auquel cas les services peuvent être la consultation d'un ou plusieurs comptes, le transfert d'argent, les paiements, les retraits, etc. Un autre fournisseur pourrait être un fournisseur d'accès à des événements de télévision à péage ou à d'autres événements tels que des nouvelles, des informations boursières, la météo,...

[0022] Le procédé de l'invention peut également être utilisé pour accéder à des services proposés par un appareil tel qu'une tablette, une voiture, etc. Dans ce cas, le module d'authentification est intégré au dispositif ou à l'appareil offrant le service requis.

[0023] Avant de démarrer une procédure d'authentification, le module d'authentification requiert généralement une identification de l'utilisateur. Ceci permet à ce module de déterminer quelles sont les données et les paramètres à utiliser pour authentifier l'utilisateur. Cette identification peut se faire par exemple en demandant à l'utilisateur d'introduire un nom (user name) ou un code personnel (PIN code). Bien entendu, d'autres manières d'identifier un utilisateur peuvent être envisagées.

[0024] Dans le cas où le fournisseur ou l'appareil donne accès à plusieurs services différents, il est possible que ce fournisseur ou cet appareil demande à l'utilisateur d'indiquer en premier lieu, le service auquel il souhaite accéder. Il est également possible que le fournisseur d'accès ou l'appareil demande cette information dans un deuxième temps uniquement ou qu'il ne le demande pas du tout.

[0025] Lorsque l'utilisateur s'est identifié, le module d'authentification peut par exemple indiquer à l'utilisateur quels sont les services auxquels il pourrait avoir accès pour autant qu'une authentification réussisse.

[0026] Si le module d'authentification demande à quel service l'utilisateur souhaite accéder, cet utilisateur entre sa réponse par exemple au moyen de l'interface. Si le module d'authentification ne demande pas à quel service l'utilisateur souhaite accéder, l'interface acquiert une première donnée d'authentification correspondant à l'utilisateur. Cette première donnée d'authentification peut être par exemple un mot de passe tapé sur un clavier par l'utilisateur. Elle peut également être une donnée biométrique telle qu'une image de la rétine de l'utilisateur, etc. La première donnée d'authentification peut également être une combinaison de plusieurs éléments, par exemple une réponse à un calcul que l'utilisateur doit prononcer à haute voix, ce calcul pouvant être affiché à l'écran ou résulter d'une règle secrète convenue entre le fournisseur de services et l'utilisateur. Dans ce cas, la reconnaissance vocale peut être utilisée comme donnée d'authentification, éventuellement en plus de la règle secrète.

[0027] Cette donnée d'authentification initiale, de même que toutes les autres données d'authentification, est associée à au moins deux valeurs, l'une des valeurs étant associée à l'introduction correcte de la donnée d'authentification et l'autre valeur étant associée à l'introduction incorrecte de cette donnée d'authentification. Il est à noter que ces valeurs ne sont pas nécessairement statiques. Selon un mode de réalisation préféré, la valeur associée à l'introduction correcte de la donnée d'authentification est positive. La valeur associée à l'introduction incorrecte de la donnée d'authentification peut être nulle ou négative par exemple. Elle pourrait être positive, mais moins grande que la valeur associée à l'introduction d'une valeur d'authentification correcte.

[0028] Selon une variante, une donnée d'authentification est associée à plus de deux valeurs. Ceci pourrait être le cas d'une donnée d'authentification utilisant le comportement de l'utilisateur. Ce comportement n'étant pas strictement reproductible d'une fois à l'autre, différentes valeurs peuvent être associées à la donnée d'authentification, avec comme règle que plus le comportement mesuré lors d'une tentative de connexion s'éloigne du comportement mémorisé par le module d'authentification, plus la valeur attribuée est faible. Plusieurs valeurs pourraient également être associées à un mot de passe ou une phrase secrète, ce qui permettrait, dans une certaine mesure, d'accepter qu'un utilisateur introduise un mot de passe ou une phrase secrète avec une faute de frappe. Le fait d'avoir plusieurs valeurs associées à une donnée d'authentification est particulièrement intéressant dans les cas où les données d'authentification sont des données biométriques. Généralement, lors de l'utilisation de données biométriques, un nombre relativement important d'éléments sont mesurés et une correspondance est recherchée entre les éléments mesurés et les données correspondantes mémorisée pour l'utilisateur concerné. Dans les systèmes de l'art antérieur, une valeur limite est fixée. Si, pour un nombre de

points supérieur à la valeur limite, les éléments mesurés et les données mémorisées concordent, l'authentification est considérée comme correcte. Si le nombre de données concordantes est inférieur à la valeur limite, l'authentification est considérée comme incorrecte.

[0029] Dans la présente invention, il est possible d'attribuer une valeur dépendant du nombre de points de concordance, selon une échelle beaucoup plus fine que dans les systèmes existants.

[0030] L'association entre une donnée d'authentification et une valeur d'authentification peut se faire de différentes façons. Par exemple, il est possible de définir une valeur fixe par type de donnée d'authentification. Généralement, plus le type de données d'authentification est facile à falsifier, plus la valeur est faible. Ainsi, un mot de passe aura généralement moins de valeur qu'une donnée biométrique. Dans le cas de l'attribution d'une valeur fixe par type de donnée, un mot de passe aura toujours la même valeur quel que soit le mot de passe.

[0031] Il est également possible d'attribuer une valeur ne dépendant pas uniquement du type de donnée, mais également de la donnée elle-même. Dans ce cas là, un mot de passe court tiré du vocabulaire courant aura une valeur moins grande qu'un mot de passe long comprenant des majuscules et des minuscules, des caractères particuliers et des chiffres.

[0032] La valeur d'authentification pour une donnée d'authentification déterminée peut également dépendre d'autres paramètres tels que par exemple l'heure du jour et/ou le jour de la semaine. Un même mot de passe permettant par exemple l'accès à des services de paiement destinés à des entreprises, pourrait ainsi avoir une valeur élevée pendant les heures d'ouverture de l'entreprise et une valeur plus faible en dehors de ces périodes. Ceci permet de tenir compte du fait qu'une demande d'accès au service en dehors des heures ouvrables a plus de risques d'être le fait d'un usurpateur que la même demande d'accès pendant les heures d'ouverture de l'entreprise. Ces heures d'ouverture pourraient être définies par l'entreprise elle-même, de façon individualisé et ne serait pas nécessairement commune à tous les services et tous les utilisateur de services d'un fournisseur déterminé. La valeur d'authentification peut également dépendre de l'historique de l'utilisateur ou de la demande d'accès. Ainsi, l'introduction pour la première fois, d'un mot de passe faux pourrait être associée à une première valeur négative. L'introduction pour la deuxième fois lors de la même demande d'accès, d'un mot de passe faux pourrait être associée à une deuxième valeur négative, différente de la première valeur et ayant une valeur absolue plus grande que celle de la première valeur.

[0033] Selon une variante, un poids pourrait être associé aux tentatives de connexion échouées. Ainsi, un poids de 1 pourrait par exemple être associé à l'introduction d'une première donnée d'authentification fausse, un poids de 1.2 à l'introduction d'une deuxième donnée d'authentification fausse et un poids de 1.5 à l'introduction d'une troisième donnée d'authentification fausse.

[0034] Selon la méthode de l'invention, lorsque l'interface a acquis une donnée d'authentification, le module d'authentification attribue une valeur d'authentification à cette donnée. Pour ceci, le module d'authentification détermine quels sont les différentes valeurs possibles pour cette donnée d'authentification, quelles sont les conditions associées à ces valeurs possibles et quelle condition spécifique, la donnée d'authentification introduite par l'utilisateur rempli.

[0035] Selon un mode de réalisation simple, les conditions peuvent être l'attribution de la valeur maximale si la donnée d'authentification introduite est identique à la donnée d'authentification mémorisée ou attendue par le module d'authentification et une valeur nulle dans le cas contraire.

[0036] Le module d'authentification détermine ensuite quelle valeur de seuil doit être atteinte pour accéder au service requis par l'utilisateur. Ce seuil est mémorisé par le module d'authentification est peut être fixe pour un service ou au contraire dépendre de différents paramètres. Ces paramètres peuvent être par exemple une période dans la journée ou certains jours de la semaine. Ils peuvent également tenir compte du lieu à partir duquel un utilisateur souhaite accéder à un service. Le lieu d'où provient la demande d'accès pourrait également être considéré comme une donnée d'authentification.

[0037] Dans l'étape suivante de la méthode, le module d'authentification vérifie si la valeur d'authentification initiale atteinte par l'utilisateur est supérieure ou égale à la valeur de seuil pour le service considéré. Si la réponse à cette question est positive, l'accès au service est autorisé.

[0038] Si la réponse à cette question est négative, la méthode se poursuit par la recherche d'une donnée d'authentification supplémentaire pour cet utilisateur. Le module d'authentification dispose, pour chaque utilisateur, d'un répertoire des données d'authentification disponibles. De plus, les données d'authentification qui ont déjà été utilisées lors de la procédure de connexion en cours sont marquées comme non disponibles ou utilisées. Le module d'authentification est donc en mesure de savoir si d'autres données d'authentification sont disponibles pour l'utilisateur en question.

[0039] Si aucune donnée d'authentification supplémentaire n'est disponible et que la valeur d'authentification n'a pas atteint le seuil, l'accès au service est refusé. Si au contraire, une ou des données d'authentification supplémentaires sont disponibles, l'interface acquiert une telle donnée d'authentification. Cette acquisition se fait de manière similaire à l'acquisition de la donnée d'authentification initiale.

[0040] Il est à noter que si plusieurs données d'authentification sont disponibles, plusieurs variantes sont envisageables. Selon une variante, l'utilisateur choisi quelle donnée d'authentification il souhaite utiliser. Selon une autre variante, un ordre d'utilisation est défini et le module d'authentification s'en tient à cet ordre. Selon une autre variante, le module d'authentification choisi une donnée

d'authentification supplémentaire qui permettra à l'utilisateur d'accéder au service si l'authentification est réussie, mais qui aura la valeur d'authentification la plus faible possible pour permettre l'accès à ce service. Ceci peut être intéressant du fait qu'en principe, plus une donnée d'authentification a une valeur d'authentification élevée, plus elle sera intéressante à intercepter pour un usurpateur. Il est donc judicieux d'utiliser, et potentiellement de divulguer, une information ayant la valeur la plus faible possible pour atteindre le but recherché, à savoir accéder à un service déterminé. Dans ce contexte là, il est également possible d'indiquer à l'utilisateur quelle est la valeur d'authentification qu'il a atteint, quelle valeur de seuil il doit atteindre et quelles sont les valeurs d'authentification des différentes données d'authentification dont il dispose. Ainsi, il pourra choisir au mieux, la donnée d'authentification qu'il utilisera.

[0041] Lorsque cette donnée d'authentification est choisie et acquise par le module d'authentification au moyen de l'interface, une valeur d'authentification lui est attribuée comme précédemment. Cette valeur est nommée ici valeur d'authentification supplémentaire. Cette valeur d'authentification supplémentaire est combinée à la valeur d'authentification mémorisée, qui correspond à la valeur d'authentification initiale.

[0042] La combinaison pourrait être simplement l'addition des deux valeurs. Cette addition n'est toutefois pas la seule solution possible. Il est par exemple possible d'ajouter un "poids" à chaque valeur d'authentification. Le poids pourrait être de 1 pour la valeur initiale, de 0.9 pour la première valeur supplémentaire, 0.8 pour la deuxième valeur supplémentaire, etc.. Il est clair que l'invention n'est pas limitée aux combinaisons décrites ici.

[0043] Le résultat de cette combinaison est nommé valeur d'authentification combinée, cette valeur étant mémorisée soit à la place de la valeur d'authentification initiale, soit en plus de cette valeur. La valeur d'authentification combinée est comparée à la valeur de seuil. Si le seuil est atteint ou dépassé, l'accès au service est autorisé. Sinon, comme précédemment, le module d'authentification détermine s'il dispose encore de données d'authentification supplémentaires pour cet utilisateur.

[0044] La méthode se poursuit ainsi, en combinant à chaque tour, la valeur d'authentification mémorisée et la valeur d'authentification supplémentaire. Cette méthode prend fin soit lorsque la valeur d'authentification combinée atteint ou dépasse le seuil, soit lorsque toutes les données d'authentification disponibles pour cet utilisateur ont été utilisées, sans que la valeur de seuil soit atteinte.

[0045] Il est également possible de limiter le nombre de tours de la méthode en imposant un nombre maximal de données d'authentification par tentative de connexions. Ainsi, même si le module d'authentification dispose par exemple de cinq données d'authentification ou cinq secrets pour un utilisateur donné, un maximum de trois données peuvent être utilisées pour l'accès au service. Si le seuil n'est pas atteint après l'utilisation de ces trois données d'authentification, l'accès est refusé

[0046] Selon un exemple concret illustré par la figure 2, supposons que l'utilisateur ait à sa disposition quatre éléments associés à des données d'authentification, à savoir :

- une carte à puce associée à une valeur de 60 lorsque cette carte donne un résultat correct et une valeur de -10 si la carte donne un résultat erroné;
- un mot de passe correspondant à une valeur de 30 lorsqu'il est introduit correctement et de zéro s'il est introduit de façon incorrecte;
- une donnée biométrique associée à la reconnaissance faciale de l'utilisateur, cette donnée étant associée à une valeur de 70 si la reconnaissance vocale est totalement réussie, de zéro si elle est partiellement réussie et de -50 si l'authentification échoue; et
- une règle secrète, consistant pour l'utilisateur, à multiplier par 4, la valeur que le fournisseur indique à l'utilisateur. Cette règle secrète est associée à une valeur de 55 si la réponse de l'utilisateur est juste et de -10 si elle est fausse

[0047] Dans un premier exemple d'utilisation de l'invention, le fournisseur de services propose deux services. L'accès au premier service est autorisé dès le moment où la valeur d'authentification dépasse un seuil fixé, par exemple 80. Le seuil pour la valeur d'authentification permettant d'accéder au deuxième service est fixé à 120 dans notre exemple.

[0048] Selon cet exemple de réalisation, lorsque l'utilisateur souhaite accéder au service, le module d'authentification indique à l'utilisateur qu'il doit fournir une donnée d'authentification. Selon l'implémentation, l'utilisateur peut avoir le choix du type de donnée qu'il souhaite introduire ou au contraire, ce choix peut être imposé par le module d'authentification.

[0049] Supposons ici que le choix soit laissé à l'utilisateur et que ce dernier choisisse d'utiliser la carte à puce. Si les données lues à partir de la carte à puce par l'interface correspondent aux données attendues par le module d'authentification, une valeur d'authentification initiale de 60 est attribuée à cet utilisateur. Cette valeur d'authentification initiale est comparée à la valeur de seuil, qui est de 80 dans l'exemple considéré, pour le premier service. La valeur d'authentification initiale est inférieure à la valeur de seuil. L'accès au premier service n'est alors pas autorisé à ce stade.

[0050] Le module d'authentification vérifie ensuite si une autre donnée d'authentification est disponible pour cet utilisateur. Cette autre donnée peut être un mot de passe ou toute autre donnée d'authentification, mais doit bien entendu être différent de la donnée d'authentifica-

tion déjà utilisée. Pour ceci, les données d'authentification déjà utilisées lors d'une tentative de connexion sont marquées comme utilisées ou non disponibles.

[0051] Dans l'exemple décrit, trois autres données d'authentification sont disponibles, à savoir un mot de passe, une règle secrète et une donnée biométrique. Selon un premier mode de réalisation, l'utilisateur a le choix du type de données qu'il souhaite utiliser parmi les données possibles non encore utilisées. Selon un deuxième mode de réalisation, le module d'authentification impose le type de données. Dans un mode de réalisation avantageux, le module d'authentification imposera le type de données qui a la valeur la plus faible possible pour atteindre la valeur de seuil.

[0052] Dans notre exemple, l'utilisateur utilisera le mot de passe. Si ce mot de passe est introduit correctement et correspond à ce qui est attendu par le module d'authentification, une valeur d'authentification supplémentaire est attribuée à l'utilisateur. Dans l'exemple, cette valeur est de 40.

[0053] La valeur d'authentification initiale (60) et la valeur d'authentification supplémentaire (40) sont combinées. Dans le cas d'une combinaison correspondant à une addition, le résultat de la combinaison est dénommé valeur d'authentification combinée et serait de 60 + 40 = 100, selon l'exemple.

[0054] Cette valeur d'authentification combinée est comparée à la valeur de seuil qui est de 80 dans l'exemple. La valeur d'authentification combinée est supérieure à la valeur de seuil. Il en résulte que l'accès au premier service est autorisé.

[0055] Il va de soi que qu'il est possible de définir que l'accès au service est autorisé dès que la valeur de seuil est atteinte ou au contraire, d'imposer que cette valeur de seuil soit dépassée.

[0056] Si l'utilisateur souhaite accéder au deuxième service, qui requiert une valeur d'authentification supérieure ou égale à 120, il pourra par exemple utiliser la règle secrète, qui consiste à multiplier par 4, la valeur affichée sur l'interface. Dans l'exemple considéré, illustré par la figure 2, imaginons que l'utilisateur introduise un résultat erroné en réponse à la règle secrète. Ce résultat erroné est associé à une valeur de -50. En reprenant le cas où la combinaison est une adition des valeurs d'authentification, la valeur d'authentification combinée sera de 100 - 50 = 50. Cette valeur étant inférieure à la valeur de seuil pour le deuxième service, l'utilisateur n'y aura pas accès.

[0057] Il est à noter que la valeur obtenue est également inférieure à la valeur de seuil pour le premier service. Dans ce cas, plusieurs variantes sont possibles. Dans une première variante, comme l'utilisateur avait accès précédemment au premier service, aussi longtemps que cet utilisateur ne se déconnecte pas, la valeur de seuil du premier service n'est pas contrôlée et l'utilisateur continue d'avoir accès à ce premier service.

[0058] Dans une autre variante, la valeur de seuil est contrôlée lors de chaque utilisation d'une donnée d'authentification. Comme la valeur d'authentification combinée (50) est inférieure à la valeur de seuil (80) pour le premier service, l'accès à ce service est désactivé et l'utilisateur doit utiliser une nouvelle donnée d'authentification pour accéder aux services, que ce soit le premier ou le deuxième service.

[0059] Dans l'exemple choisi, le module d'authentification dispose encore d'une donnée d'authentification disponible pour cet utilisateur, à savoir une donnée biométrique. L'utilisateur qui choisit d'accéder au deuxième service laisse l'interface acquérir les données biométriques. Si l'authentification se fait de façon correcte, la valeur d'authentification de ces données biométriques, qui est de 70 dans l'exemple. La combinaison de la valeur d'authentification supplémentaire liée à la donnée biométrique avec la valeur d'authentification combinée mémorisée, liée aux trois autres données utilisées, donne une valeur de 50 + 70 = 120. Cette valeur d'authentification combinée est égale au seuil de 120 permettant d'accéder au deuxième service. L'accès est donc autorisé à cet utilisateur.

[0060] Comme on peut le voir dans cet exemple, il est possible que l'utilisateur soit autorisé à accéder à un service malgré le fait qu'au moins une des données d'authentification ne corresponde pas au résultat attendu. Comme on peut également le voir de cet exemple, les valeurs d'authentification sont mémorisées lors du déroulement de la méthode.

[0061] Les données d'authentification ou les secrets déjà utilisés ne peuvent plus être utilisés lors de cette connexion à un service, faute de quoi il serait possible d'atteindre n'importe quelle valeur en introduisant une même donnée, par exemple un mot de passe correct, un nombre suffisant de fois. Une donnée d'authentification déjà utilisée de façon correcte est donc marquée comme telle. Une donnée d'authentification que l'utilisateur a cherché à utiliser, sans succès, par exemple un mot de passe incorrect, peut être marquée comme inutilisable pour cette tentative de connexion. Elle peut également ne pas être marquée ou marquée comme utilisable. Dans ce cas, l'utilisateur peut tenter autant de fois qu'il le souhaite, d'utiliser la donnée d'authentification. Finalement, selon un mode de réalisation préféré, chaque tentative d'utiliser une donnée d'authentification est mémorisée et le nombre de tentatives pendant une session de connexion est limité, par exemple à trois. Si après trois tentatives échouées, la donnée d'authentification n'a pas pu être utilisée, selon l'implémentation choisie, l'accès aux services est bloqué, même si d'autres données d'authentification sont encore disponibles, ou au contraire, uniquement l'utilisation de la donnée d'authentification ayant conduit à un échec est bloquée, les autres données d'authentification étant encore utilisables.

[0062] Il est à noter qu'un mélange de ces variantes est possible. Par exemple, pour la consultation de comptes bancaires, trois erreurs de code PIN entraînent une interdiction d'utiliser ce code PIN pendant la connexion en cours, cette connexion étant toujours possible au

moyen d'une carte à puce. Par contre, pour les retraits d'argent d'une somme supérieure à X, trois erreurs aboutissent à un blocage de la connexion.

[0063] Supposons maintenant que l'utilisateur qui cherche à accéder à un service introduise d'abord une carte à puce reconnue comme valide, puis le mot de passe de façon erronée. Dans cet exemple, le mot de passe erroné est associé à une valeur de -50. Le module d'authentification, lors de la vérification de l'existence de données d'authentification supplémentaires pour cet utilisateur constatera qu'il dispose bien de données d'authentification. Supposons que l'utilisateur introduise un résultat faux lors de l'utilisation de la règle secrète. La valeur d'authentification combinée sera de 60 - 50 - 50 =-40, en appliquant les principes décrits ci-dessus. Le module d'authentification vérifiera s'il dispose d'autres données d'authentification. Dans un premier mode de réalisation, le module d'authentification demandera à l'utilisateur d'utiliser ces données en introduisant des données d'authentification supplémentaires. Dans un deuxième mode de réalisation avantageux, avant de demander à l'utilisateur d'introduire des données d'authentification supplémentaires, le module d'authentification vérifiera si la combinaison de la valeur d'authentification combinée actuelle (-40) et de la valeur d'authentification que l'utilisateur peut obtenir avec toutes les données d'authentification dont dispose ce module d'authentification (70), est suffisante pour atteindre la valeur de seuil. Si tel n'est pas le cas, il indiquera à l'utilisateur que l'accès au service est refusé.

[0064] Dans l'exemple ci-dessus, l'utilisateur a une valeur d'authentification combinée actuelle de -40. Le module d'authentification dispose d'une seule donnée d'authentification pour cet utilisateur, dont la valeur est de 70. Quelle que soit la valeur obtenue lors de l'authentification utilisant cette donnée supplémentaire, la valeur d'authentification combinée n'atteindra pas la valeur de seuil et l'accès sera refusé. Il est donc d'une part inutile et d'autre part risqué, de demander à l'utilisateur d'introduire la dernière donnée d'authentification. En effet, cette donnée pourrait être mémorisée par un usurpateur.

[0065] Selon un mode de réalisation concret, si le fournisseur de services est par exemple un établissement financier, un premier seuil pour un premier service pourrait être associé à la consultation des comptes de l'utilisateur. Un deuxième seuil, généralement plus élevé que le premier seuil pourrait être associé à des transferts d'un compte de l'utilisateur à un autre compte du même utilisateur. Un troisième seuil pourrait être associé à des paiements d'un montant inférieur à une certaine somme et enfin un quatrième seuil pourrait être associé à des paiements supérieurs à cette somme.

[0066] Dans le cas où le fournisseur est un fournisseur d'événements de télévision à péage par exemple, un premier seuil pourrait être associé à l'accès à un canal ou un ensemble de canaux déterminés et un deuxième seuil pourrait être associé à un autre ensemble de canaux.

[0067] Dans ces cas, plusieurs variantes de la méthode de l'invention peuvent être utilisées. Selon une première variante, l'utilisateur doit indiquer, par exemple avant d'introduire la première donnée d'authentification, à quel service il souhaite accéder. Il peut également indiquer le service juste après l'introduction de la première donnée d'authentification, avant l'introduction de la donnée d'authentification supplémentaire. La suite du procédé se déroule de la même manière que ce qui a été décrit précédemment, le seuil utilisé dépendant du service auquel l'utilisateur souhaite accéder.

[0068] Selon une deuxième variante, l'utilisateur n'indique pas à quel service il souhaite accéder, mais le module d'authentification indique une liste des services auxquels l'utilisateur peut accéder en fonction de la valeur d'authentification combinée atteinte. Cette liste peut augmenter au fur et à mesure que l'utilisateur introduit des données d'authentification correctes ou au contraire, diminuer si des données incorrectes sont introduites. L'utilisateur peut arrêter d'introduire des données d'authentification dès lors que le service auquel il souhaite accéder est disponible.

[0069] Le module d'authentification peut également indiquer à l'utilisateur tous les services proposés, cette indication se faisant sous la forme de deux listes. L'une des listes peut comporter les services auxquels l'utilisateur a accès, en particulier en tenant compte de la valeur d'authentification combinée atteinte par l'utilisateur et l'autre liste contenant les services auxquels l'utilisateur n'a pas accès. Les listes peuvent être distinguées par des couleurs, par exemple vert pour les services accessibles et rouge pour les autres ou noir pour les services accessibles et gris pour les autres.

[0070] Il est à noter que les données d'authentification, ainsi que les services proposés, ne sont pas nécessairement communiqués par le module d'authentification. Il en découle la possibilité pour ce dernier de collecter des données d'authentification (notamment de type "comportement" ou biométrique) à l'insu de l'utilisateur et d'utiliser ensuite ces données pour élaborer la valeur d'authentification.

[0071] Selon une variante, la valeur combinée acquise par l'utilisateur lors d'une session est mémorisée. Ainsi, si l'utilisateur a introduit suffisamment de données d'authentification pour consulter ses comptes dans un établissement bancaire, sans toutefois être autorisé à faire un paiement, il devra introduire des données d'authentification additionnelles lorsqu'il souhaitera faire un paiement.

[0072] Selon une autre variante, l'accès à un service pourrait être accordé à un utilisateur dès lors que la valeur d'authentification a atteint le seuil, mais le comportement du fournisseur de services pourrait être différent en fonction de cette valeur d'authentification. A titre d'exemple, l'accès à un service pourrait être accordé dès lors que la valeur d'authentification a atteint 50. Toutefois, si la valeur d'authentification n'a pas dépassé 80, des informations par exemple relatives aux opérations effectuées ou à un lieu ou une adresse logique à partir desquelles

les opérations sont effectuées, sont mémorisées.

[0073] La présente invention propose plusieurs variantes pour la gestion de l'authentification d'un utilisateur. Ces variantes peuvent être combinées entre elles.

[0074] Cette invention offre une grande souplesse, ce qui permet à l'utilisateur d'avoir accès à des services selon une procédure qui lui convient le mieux.

[0075] Cet utilisateur peut également paramétrer dans une certaine mesure, le niveau de sécurité qu'il souhaite avoir. Ainsi, si le fournisseur impose une valeur minimale de 80 pour l'accès à un certain service, l'utilisateur pourra définir que, pour ce service spécifique, la valeur d'authentification combinée doit être 90 au lieu de 80. Etant donné que dans ce cas, c'est l'utilisateur qui choisit d'augmenter le niveau de sécurité, il sera prêt à accepter une diminution de la facilité d'usage qui en résulte généralement.

[0076] Il est également possible de prévoir que le fournisseur définisse une certaine plage, par exemple entre 70 et 90, qu'il fixe par défaut une certaine valeur, par exemple 80 et que l'utilisateur puisse préciser la valeur qu'il souhaite utiliser, dans la plage de valeurs définie par le fournisseur.

[0077] Dans les différents exemples et modes de réalisation décrits ci-dessus, il est possible d'afficher, à l'attention de l'utilisateur, les valeurs d'authentification. Ainsi, il est par exemple possible à chaque instant, d'afficher la valeur d'authentification actuelle ainsi que la valeur d'authentification de chaque donnée disponible pour cet utilisateur. Au contraire, il est également possible de ne rien afficher et d'avoir une méthode d'authentification totalement transparente pour l'utilisateur. Il est également possible d'afficher uniquement une partie des informations liées à l'authentification.

Revendications

1. Méthode d'authentification d'un utilisateur par un module d'authentification, ledit module d'authentification gérant l'accès à une pluralité de services et comprenant un seuil d'authentification pour chaque service, au moins deux données d'authentification étant associées audit utilisateur, ladite méthode comprenant les étapes suivantes :

   a) acquisition d'au moins une donnée d'authentification de l'utilisateur, au moyen d'une interface entre cet utilisateur et ledit module d'authentification;
   b) vérification de ladite au moins une donnée d'authentification et attribution d'une valeur d'authentification à l'utilisateur, en fonction du résultat de la vérification;
   c) comparaison de la valeur d'authentification avec la valeur de seuil pour le service requis;
   d) si la valeur d'authentification est égale ou supérieure à la valeur de seuil, accorder l'accès au service requis par l'utilisateur;
   e) si la valeur d'authentification est inférieure à la valeur de seuil, vérification si une donnée d'authentification non utilisée est disponible pour cet utilisateur;
   f) si aucune donnée d'authentification non utilisée n'est disponible pour cet utilisateur, refus de l'accès au service requis;
   g) si au moins une donnée d'authentification non utilisée est disponible pour cet utilisateur, répétition des étapes a) à f) en acquérrant une donnée d'authentification différente de celle(s) présentée(s) antérieurement et en combinant les valeurs d'authentification, ladite comparaison étant faite entre la valeur de seuil et la combinaison des valeurs d'authentification.

2. Méthode d'authentification selon la revendication 1, **caractérisée en ce que** la valeur d'authentification attribuée à une donnée d'authentification dépend de la concordance entre la donnée d'authentification acquise par ladite interface et la donnée d'authentification correspondante mémorisé par ledit module d'authentification.

3. Méthode d'authentification selon la revendication 1, **caractérisée en ce que** la combinaison des valeurs d'authentification est une addition desdites valeurs d'authentification.

4. Méthode d'authentification selon la revendication 1, **caractérisée en ce que** chaque donnée d'authentification est associée à au moins deux valeurs d'authentification distinctes.

5. Méthode d'authentification selon la revendication 4, **caractérisée en ce que** l'une des valeurs d'authentification associée à une donnée d'authentification est attribuée en cas d'identité entre la donnée d'authentification acquise par l'interface et la donnée d'authentification correspondante mémorisée par le module d'authentification, une autre des valeurs d'authentification étant attribuée en cas de différence entre la donnée d'authentification acquise par l'interface et la donnée d'authentification correspondante mémorisée par le module d'authentification.

6. Méthode d'authentification selon la revendication 1, **caractérisée en ce que** les données d'authentification sont associées à au moins trois valeurs d'authentification distinctes, et **en ce que** plus il y a de différences entre une donnée d'authentification acquise par l'interface et la donnée d'authentification correspondante mémorisée par le module d'authentification, plus la valeur d'authentification attribuée est basse.

7. Méthode d'authentification selon la revendication 1,

caractérisée en ce que chaque service étant associé à une valeur de seuil différente.

8. Méthode d'authentification selon la revendication 1, **caractérisée en ce que** le module d'authentification indique à l'utilisateur la donnée d'authentification que cet utilisateur doit utiliser.

9. Méthode d'authentification selon la revendication 8, **caractérisée en ce que** le module d'authentification choisi, en fonction du seuil correspondant au service requis par l'utilisateur et en fonction de la valeur d'authentification atteinte par l'utilisateur, le service ayant la valeur d'authentification la plus faible possible permettant l'accès audit service.

10. Méthode d'authentification selon la revendication 1, **caractérisée en ce que** le module d'authentification indique à l'utilisateur au moins la valeur de seuil pour l'accès audit service, la valeur d'authentification combinée atteinte par l'utilisateur et la valeur d'authentification des données d'authentification non utilisées, disponibles pour ledit utilisateur.

11. Méthode d'authentification selon la revendication 1, **caractérisée en ce qu'**au moins trois données d'authentification sont associées audit utilisateur et dans laquelle ledit utilisateur peut accéder à un service soit en utilisant une seule donnée d'authentification parmi lesdites au moins trois données d'authentification, soit en utilisant au moins deux autres données d'authentification parmi les données d'authentification différentes de la donnée d'authentification permettant à elle seule, l'accès audit service.

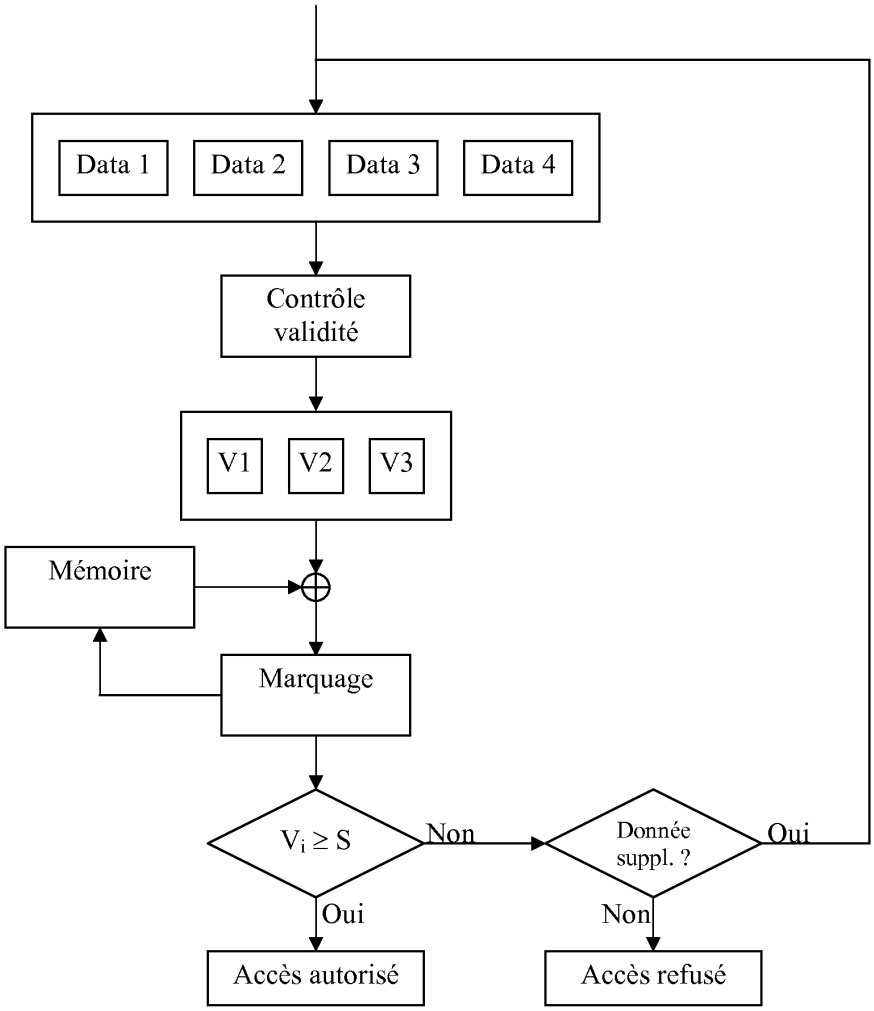
Data 1
Data 2
Data 3
Data 4
Contrôle validité
V1
V2
V3
Mémoire
Marquage
$V_i \geq S$
Non
Donnée suppl. ?
Oui
Oui
Non
Accès autorisé
Accès refusé

Fig. 1

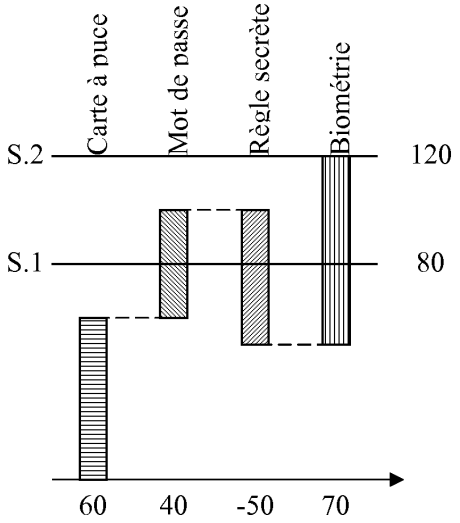
Carte à puce
Mot de passe
Règle secrète
Biométrie
S.2
120
S.1
80
60
40
-50
70

Fig. 2

Europäisches Patentamt
European Patent Office
Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 13 19 2404

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (IPC)
X	WO 2009/097179 A1 (FIRST DATA CORP [US]; WAGNER THERESA LYNN [US]; PINKERTON PEGGY ANN [U) 6 août 2009 (2009-08-06) * alinéa [0009] - alinéa [0010] * * alinéa [0033] * * alinéa [0035] - alinéa [0038] * * alinéa [0057] * * alinéa [0061] * -----	1-11	INV. G07C9/00
A	US 2007/177768 A1 (TSANTES GEORGE K [US] ET AL) 2 août 2007 (2007-08-02) * alinéa [0010] * * alinéa [0029] * -----	1	
A	US 2004/189441 A1 (STERGIOU KOSMAS [US]) 30 septembre 2004 (2004-09-30) * revendications 1-2 * * revendications 15-16 * -----	1,2,7	
			DOMAINES TECHNIQUES RECHERCHES (IPC)
			G07C

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
La Haye	25 avril 2014	Ngandu, William

CATEGORIE DES DOCUMENTS CITES

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 antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C02)

ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE RELATIF A LA DEMANDE DE BREVET EUROPEEN NO. EP 13 19 2404

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche européenne visé ci-dessus.
Lesdits members sont contenus au fichier informatique de l'Office européen des brevets à la date du
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

25-04-2014

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 2009097179 A1	06-08-2009	US 2009198587 A1 WO 2009097179 A1	06-08-2009 06-08-2009
US 2007177768 A1	02-08-2007	AUCUN	
US 2004189441 A1	30-09-2004	AUCUN	

EPO FORM P0460

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82