ROYAUME DU MAROC

OFFICE MAROCAIN DE LA PROPRIETE INDUSTRIELLE ET COMMERCIALE
---

(19)

المملكة المغربية

المكتب المغربي للملكية الصناعية و التجارية
---

(12) FASCICULE DE BREVET

(11) N° de publication :
MA 31107 B1

(51) Cl. internationale :
G06F 21/20

(43) Date de publication :
04.01.2010

(21) N° Dépôt :
32113

(22) Date de Dépôt :
23.07.2009

(30) Données de Priorité :
23.01.2007 FR 0752843

(86) Données relatives à l'entrée en phase nationale selon le PCT :
PCT/FR2008/050104 23.01.2008

(71) Demandeur(s) :
NCRYPTONE, 150 RUE GALLIENI F-92100 BOULOGNE BILLANCOURT (FR)

(72) Inventeur(s) :
BLOT, Philippe ; RENAUD, Jean-Charles ; BUSCHINI, Philippe

(74) Mandataire :
CABINET ABDERRAZIK

(54) Titre : **DISPOSITIF PORTABLE D'AUTHENTIFICATION.**

(57) Abrégé : L'INVENTION SE RAPPORTE À UN DISPOSITIF (10) PORTABLE D'AUTHENTIFICATION D'UN UTILISATEUR, COMPRENANT UN BOÎTIER (101) UNIQUE DANS LEQUEL SONT LOGÉS : - DES MOYENS (16) D'ACTIVATION DU DISPOSITIF, TELLE QU'UNE TOUCHE DEVANT ÊTRE PRESSÉE PAR L'UTILISATEUR; - UN MICROPROCESSEUR (32) EFFECTUANT UN CALCUL LORS DE L'ACTIVATION DU DISPOSITIF (10), LE CALCUL METTANT EN ¿UVRE UN ALGORITHME BASÉ SUR UNE CLÉ SECRÈTE STOCKÉE DANS UNE MÉMOIRE (37), ET AYANT POUR RÉSULTAT UN MOT DE PASSE DYNAMIQUE; LE DISPOSITIF (10) ÉTANT TEL QUE LA MÉMOIRE (37) DANS LAQUELLE EST STOCKÉE LA CLÉ SECRÈTE EST DISPOSÉE À L'INTÉRIEUR DU BOÎTIER (101) ET CONNECTÉE AU DISPOSITIF DE MANIÈRE AMOVIBLE.

ABREGE

L'invention se rapporte à un dispositif (10) portable d'authentification d'un utilisateur, comprenant un boîtier (10_1) unique dans lequel sont logés : - des moyens (16) d'activation du dispositif, telle qu'une touche devant être pressée par l'utilisateur; - un microprocesseur (32) effectuant un calcul lors de l'activation du dispositif (10), le calcul mettant en œuvre un algorithme basé sur une clé secrète stockée dans une mémoire (37), et ayant pour résultat un mot de passe dynamique; le dispositif (10) étant tel que la mémoire (37) dans laquelle est stockée la clé secrète est disposée à l'intérieur du boîtier (10_1) et connectée au dispositif de manière amovible.

WO 2008/107607 31107 PCT/FR2008/050104

DISPOSITIF PORTABLE D'AUTHENTIFICATION

La présente invention concerne un dispositif portable et polyvalent d'authentification, permettant à un utilisateur de s'authentifier, de manière sûre et rapide, au travers de tous les canaux de communication existants (téléphone, Internet...) ou directement sur un appareil (automate, ordinateur portable...), pour accéder à tous types de services et/ou de machines sécurisés.

Pour authentifier un utilisateur d'un service ou d'une machine, telle qu'un ordinateur personnel, il est connu d'utiliser un dispositif portable fournissant un mot de passe dynamique ou « one time password » (OTP), c'est-à-dire un mot de passe différent à chaque calcul. Ce mot de passe est généré via un algorithme par un processeur, l'algorithme étant basé sur une clé secrète unique et propre au dispositif. Dans un tel dispositif, la clé secrète est implémentée via l'algorithme de calcul dans une mémoire lors de la fabrication, ce qui impose la personnalisation du dispositif dès la fabrication pour le rendre fonctionnel, de la même manière que les cartes bancaires. Une telle contrainte pose notamment des problèmes de sécurité (notamment du fait du transport de dispositifs actifs depuis leur lieu de fabrication), et ne permet pas d'effectuer de mises à jour d'amélioration et/ou de personnalisation complémentaire du dispositif, les informations contenues étant figées en usine.

L'invention part de la constatation qu'il est avantageux de pouvoir implémenter la clé secrète, entre autres informations, le plus tard possible, et en tout état de cause après fabrication (par exemple au moment de la vente), de manière simple et réversible.

Ainsi, l'invention concerne un dispositif portable d'authentification d'un utilisateur, comprenant un boîtier unique dans lequel sont logés :

- des moyens d'activation du dispositif, telle qu'une touche devant être pressée par l'utilisateur ;
- un microprocesseur effectuant un calcul lors de l'activation du dispositif, le calcul mettant en œuvre un algorithme basé sur une clé secrète stockée dans une mémoire, et ayant pour résultat un mot de passe dynamique ;

le dispositif étant tel que la mémoire dans laquelle est stockée la clé secrète est disposée à l'intérieur du boîtier et connectée au dispositif de manière amovible.

Ainsi, grâce au dispositif selon l'invention, l'utilisateur peut s'authentifier de manière sûre et rapide en fournissant à un prestataire de service et/ou à un appareil un mot de passe dynamique, c'est-à-dire différent à chaque nouvelle authentification. Le stockage de la clé secrète servant au calcul du mot de passe dynamique dans une mémoire portée par un circuit électronique amovible permet que le dispositif ne fonctionne que si ladite mémoire est correctement connectée au dispositif. L'utilisation d'une mémoire amovible procure de nombreux avantages : la personnalisation du dispositif est simplifiée car celui-ci est fabriqué en grande série et personnalisé au dernier moment, par exemple lors de la vente, par adjonction de la mémoire contenant la clé secrète. De plus, un tel dispositif offre des possibilités de personnalisation très large, notamment le choix d'activer ou non certaines fonctions. On peut également implémenter des informations complémentaires dans la mémoire et effectuer leur mise à jour. On peut ainsi faire évoluer les capacités et les fonctionnalités du dispositif sans avoir à le remplacer.

La sécurité s'en trouve également renforcée car on peut fournir à l'utilisateur les deux éléments par deux canaux distincts, ce dernier effectuant lui-même l'insertion de la mémoire contenant la clé secrète.

Dans une réalisation, la mémoire est portée par un circuit électronique, de type carte SIM ou UICC, le dispositif comprenant un connecteur pour accueillir le circuit électronique.

Dans une réalisation, le microprocesseur est porté par le même circuit électronique que la mémoire dans laquelle est stockée la clé secrète.

Dans une réalisation, le dispositif comprend un module d'émission sonore pour fournir le mot de passe dynamique sous forme de signaux acoustiques.

Dans une réalisation, le dispositif comprend un afficheur pour l'affichage du mot de passe dynamique.

Dans une réalisation, le dispositif comprend un module d'émission radiofréquences pour émettre un signal radiofréquences représentatif du mot de passe dynamique.

Dans une réalisation, le dispositif comprend une connectique de type USB et peut être connecté sur un appareil équipé d'un port de type USB.

Dans une réalisation, le dispositif comprend une batterie rechargeable, la batterie étant rechargée lorsque le dispositif est connecté via le port USB.

Dans une réalisation, la mémoire dans laquelle est stockée la clé secrète permet de stocker des informations complémentaires.

Dans une réalisation, le calcul du mot de passe dynamique prend en argument la valeur d'un compteur incrémenté à chaque nouveau calcul, et/ou dépend du temps.

Dans une réalisation, le mot de passe dynamique est simultanément fourni par le dispositif via au moins deux des moyens de communication disponibles.

Un exemple de réalisation de l'invention est décrit de manière non limitative en relation avec les figures parmi lesquelles :

- la figure 1 est un schéma en trois dimensions d'un dispositif selon l'invention,
- la figure 2 montre le dispositif de la figure 1, vu sous un angle différent,
- la figure 3 montre des composants d'un dispositif selon l'invention,
- la figure 4 montre les composants d'une variante du dispositif de la figure 3.

La figure 1 montre un dispositif 10 selon l'invention. Un tel dispositif 10 est un objet portable de dimensions réduites, formé par un boîtier unique et compact 10_1, dans l'exemple de forme sensiblement parallélépipédique. Sur une face 12 du boîtier 10_1, dite face avant, est disposé un afficheur 14, permettant l'affichage d'une séquence de caractères ou de chiffres, dans

l'exemple une séquence comprise entre six et huit caractères. Sur cette face avant 12 de l'objet portable 10 est également disposée une touche 16 constituant un moyen d'activation de l'objet portable 10. En variante, la touche 16 est remplacée par un capteur biométrique, ou par tout autre capteur apte à constituer un moyen d'activation. Le contour de la face avant 12 de l'objet portable est sensiblement rectangulaire, et l'objet 10 présente donc quatre faces latérales opposées deux à deux, deux petites faces latérales 18_1 et 18_2, et deux grandes faces latérales 20_1 et 20_2. Un élément 22 en saillie sur l'une des petites faces latérales du dispositif 18_1 comporte un trou 24 permettant d'attacher le dispositif 10, par exemple à un porte-clés.

La figure 2 montre le dispositif 10 vu sous un autre angle. On peut voir sur petite face latérale 18_2, opposée à la petite face latérale 18_1 comprenant l'élément 21, une ouverture, ou fente 26 permettant l'insertion à l'intérieur du dispositif 10 d'un circuit électronique, ou puce, par exemple de type « carte SIM ».

La figure 3 montre les composants disposés dans l'objet portable 10. Celui-ci comprend une batterie 30 pour alimenter les différents composants. Un module d'émission sonore 34, ou « buzzer » est intégré à l'objet portable. Il s'agit d'un haut-parleur de type piézoélectrique. Un microprocesseur 32 permet d'effectuer des opérations variées, parmi lesquelles le calcul d'un mot de passe dynamique, ou OTP. Le microprocesseur 32 effectue le calcul de l'OTP grâce à un algorithme basé sur une clé secrète et unique. Cette clé secrète est stockée dans une mémoire 37, connectée de manière amovible à l'objet 10, via un connecteur 38. Dans l'exemple, la mémoire 37 est portée par un circuit électronique 36 de type carte à puce, contenant un microcontrôleur et une mémoire de stockage, comme par exemple une carte de type carte SIM ou UICC (« Universal Integrated Circuit Card », carte universelle à circuit intégré). Conformément à l'invention, celle-ci est introduite dans la fente 26 et connectée au connecteur 38.

Il est avantageux d'utiliser une telle carte, car outre une mémoire de stockage, les capacités de calcul qu'elle procure permettent d'envisager d'y implémenter tout ou partie de l'algorithme de calcul du mot de passe dynamique, ainsi que des fonctions supplémentaires. Dans une variante, le microprocesseur 32 est intégré dans cette carte, et toutes les opérations de calcul effectuées par le dispositif 10 sont réalisées par la carte 36. Le dispositif

peut dans ce cas comprendre un microprocesseur (non représenté) dédié à la gestion des éléments tel que l'afficheur, le module d'émission sonore...

D'autre part, l'utilisation d'une carte de type SIM ou UICC permet d'obtenir un dispositif très compact. En effet, les dimensions d'une telle carte sont très réduites en comparaison avec une carte à puce classique au format type « carte de crédit ». Ainsi, grâce à cette taille très réduite, la carte peut être insérée intégralement et laissée à demeure dans le boîtier 10_1 (tout en restant amovible). On obtient ainsi un dispositif autonome, intégrant tous les éléments nécessaires à son fonctionnement, tout en présentant un format « de poche » comparable aux dispositifs de stockage USB (couramment appelés « clés USB »).

La carte SIM 36 peut être introduite lors de la fabrication ou à n'importe quel moment après celle-ci, notamment lors de la remise du dispositif à son utilisateur. Le dispositif n'est pas fonctionnel tant que la carte 36 n'est pas connectée à celui-ci via le connecteur 38. La fente 26 pourra être scellée après introduction de la carte SIM 36 si l'on ne souhaite pas que l'utilisateur puisse la retirer lui-même. Dans ce cas, une variante ne prévoit pas de fente ou d'ouverture sur le boîtier 10_1 du dispositif. Ainsi, l'extraction de la carte 36 peut être rendue plus difficile (en rendant nécessaire le démontage du dispositif pour accéder à la carte), voire impossible (la carte est installée lors de la fabrication et le dispositif n'est pas démontable).

Chaque mot de passe dynamique calculé est destiné à être affiché sous la forme d'une séquence de caractères alphanumériques par l'afficheur 14 et/ou émis par le buzzer 34 sous forme de signaux sonores représentatifs de ce mot de passe dynamique. L'afficheur 14 et le buzzer 34 sont deux des moyens de communication de l'OTP dont peut disposer l'objet portable 10. De préférence, les signaux émis et affichés comprennent un identifiant propre au dispositif 10 ou à la carte 36, ainsi que l'OTP.

On décrit ci-après différentes variantes de calcul et de vérification de l'OTP. Dans toutes les variantes, le mot de passe est généré via un algorithme par le microprocesseur 32, et basé sur la clé secrète, qui est originale et unique. Cette même clé est par ailleurs stockée dans une base de données d'un serveur (non montré) chargé de l'authentification, pour permettre la vérification d'un OTP fourni par un utilisateur cherchant à s'authentifier.

Dans une première variante, l'OTP est calculé via un algorithme qui prend en argument la clé secrète stockée en mémoire d'une part, et un compteur incrémenté d'une unité à chaque nouveau calcul, donc à chaque appui sur la touche 16 d'autre part. L'incrémentation du compteur fournit ainsi une valeur variable qui permet que le résultat du calcul effectué par l'algorithme soit différent à chaque calcul : on obtient ainsi un mot de passe dynamique.

Lorsque l'OTP ainsi calculé est fourni à la machine/serveur chargé de l'authentification, par exemple chez un prestataire de services à distance, celui-ci est accompagné d'un identifiant propre au dispositif 10 (et donc propre à son possesseur). Grâce à l'identifiant, le serveur extrait d'une base de donnée interne la clé secrète unique associée à l'identifiant.

Le serveur ne connaissant pas la valeur du compteur incrémental utilisée pour le calcul de l'OTP, il recherche alors la dernière valeur connue de ce compteur, c'est-à-dire celle utilisée lors de la dernière authentification, cette valeur étant stockée dans le serveur. Bien entendu, depuis cette dernière authentification effective, le dispositif aura pu être sollicité un certain nombre de fois par l'utilisateur sans utiliser les OTP calculés. Pour tenir compte de cette éventuelle différence, le serveur reproduit successivement le même calcul que celui mis en œuvre dans le dispositif, en partant de la dernière valeur connue du compteur incrémental augmentée d'une unité et en incrémentant celle-ci à chaque nouveau calcul, jusqu'à ce que le calcul donne un résultat identique à l'OTP qui a été fourni par l'utilisateur.

Par mesure de sécurité, le nombre d'itérations effectuées par le serveur sera limité, et si le serveur atteint le nombre maximum d'itérations sans avoir pu obtenir un résultat identique à l'OTP fourni, alors l'authentification est refusée. Lorsque l'OTP a été vérifié et accepté, la nouvelle valeur correcte du compteur incrémental est alors stockée dans le serveur pour servir lors de la prochaine tentative d'authentification.

Dans une deuxième variante, l'algorithme de calcul prend comme argument le compteur incrémental décrit ci-dessus et une clé dynamique variant avec le temps. On obtient cette clé dynamique grâce à un deuxième algorithme qui prend comme argument la clé secrète et une valeur T dépendant du temps. Pour obtenir une valeur T dépendant du temps de manière simple, on peut par exemple procéder de la manière suivante : on mesure le temps écoulé depuis une valeur de départ To correspondant au moment de la

personnalisation du dispositif (i.e. l'introduction initiale de la carte 36), le dispositif comprenant dans ce but une horloge. La valeur T représente alors le temps écoulé depuis To, exprimé en unités de temps. L'unité de temps utilisée est variable et peut être choisie lors de la personnalisation du dispositif (par exemple 1, 2, 5 ou 10 minutes). Pour que l'OTP puisse être vérifié par la machine ou le serveur destinataire, il faut que le référentiel temps utilisé par le dispositif soit le même que la machine/serveur destinataire. Dans ce but, la valeur de départ To introduite en mémoire lors de la personnalisation est une valeur relative permettant de synchroniser le dispositif sur le référentiel temps de la machine/serveur destinataire de l'OTP.

Dans cette deuxième variante, la vérification de l'OTP par le serveur destinataire obéit au même principe que celui décrit plus haut, en intégrant le calcul de la clé dynamique à partir de la clé secrète et de la valeur T dont le serveur dispose également.

Le dispositif selon l'invention permet de réaliser l'authentification de son possesseur au travers de tous les canaux de communication existants (téléphone, Internet...) ou directement sur un appareil (automate, ordinateur portable...). On décrit ci-après différents exemples de procédures d'authentification réalisables avec dispositif selon l'invention, lorsqu'un utilisateur doit s'identifier, auprès d'un prestataire de services ou d'une machine.

Authentification via un réseau téléphonique : c'est l'OTP sous forme de signaux sonores qui est utilisé dans ce cas. L'utilisateur presse la touche 16, et l'objet portable 10 délivre un OTP sous forme de signaux acoustiques, l'utilisateur ayant préalablement positionné son dispositif 10 à proximité du microphone du téléphone. Les signaux acoustiques sont transmis à travers le réseau téléphonique vers un serveur du prestataire concerné. Ces signaux sont alors décodés, l'identifiant est reconnu, et l'OTP est vérifié. La transaction est alors acceptée ou refusée.

Authentification via le réseau Internet : l'utilisateur est ici amené à entrer son identifiant et son OTP. Il recopie donc l'OTP tel qu'affiché par l'afficheur 14. Son identifiant et son OTP sont entrés sur un clavier d'un ordinateur connecté à un site Internet du prestataire. L'OTP est alors vérifié par le serveur du prestataire.

Authentification sur un appareil : Sur un appareil tel qu'un ordinateur portable, l'utilisateur se voit demander un identifiant et un OTP, comme pour l'authentification via un réseau.

Dans tous les cas, le prestataire de services pourra adjoindre au dispositif un code secret, tel qu'un code PIN à quatre chiffres, que l'utilisateur devra fournir en plus de l'OTP et de son identifiant, afin de renforcer la sécurité de l'authentification.

Dans une variante non représentée, l'objet portable peut être connecté via un port de type USB (« Universal Serial Bus ») à un ordinateur ou tout autre appareil équipé d'un tel port. Le dispositif comprend dans ce but une prise 40 (figure 4) adaptée au port USB. Ainsi, le dispositif peut fournir l'OTP calculé directement via le port USB.

On distingue alors deux cas : soit le mot de passe dynamique est fourni sur activation du dispositif lors de l'appui sur la touche 16, soit celui-ci est fourni en réponse à une interrogation de la machine hôte, par exemple à la demande de l'application nécessitant l'authentification. Dans ce dernier cas, l'interrogation peut être réalisée à intervalles réguliers pour augmenter la sécurité de l'application. En variante, le dispositif peut également fournir sur interrogation de la machine hôte, en complément ou en remplacement de l'OTP, un certificat électronique d'authentification (préalablement fourni par une autorité habilitée à fournir de tels certificats). Dans cette variante, le certificat est inscrit dans la mémoire 37, et ne peut être modifié ou effacé.

Dans le cas ou le dispositif est connecté via un port de type USB, la batterie 30 utilisée dans le dispositif 10 peut être de type rechargeable, celle-ci étant alors rechargée via le port USB.

Dans une autre variante non représentée, le dispositif 10 comprend également un module de communication radiofréquences 42, représenté à la figure 4, permettant de transmettre l'OTP calculé sans contact, par exemple selon les normes RFID ou NFC.

Avantageusement, le dispositif 10 comprendra tous les composants nécessaires à la mise en œuvre des différentes variantes décrites ci-dessus, mais ces fonctionnalités seront activées ou non lors de la personnalisation du dispositif. Ainsi, le prestataire de services qui fournit un tel dispositif à un client/utilisateur pourra choisir, pour ses applications propres, les fonctionnalités qu'il désire mettre en œuvre (par exemple prise en compte du temps dans le

calcul de l'OTP ou non, utilisation des radiofréquences ou non, utilisation du buzzer ou non...)

REVENDICATIONS

1. Dispositif (10) portable d'authentification d'un utilisateur, comprenant un boîtier (10_1) unique dans lequel sont logés :
   - des moyens (16) d'activation du dispositif, telle qu'une touche devant être pressée par l'utilisateur ;
   - un microprocesseur (32) effectuant un calcul lors de l'activation du dispositif (10), le calcul mettant en œuvre un algorithme basé sur une clé secrète stockée dans une mémoire (37), et ayant pour résultat un mot de passe dynamique ;

le dispositif (10) étant tel que la mémoire (37) dans laquelle est stockée la clé secrète est disposée à l'intérieur du boîtier (10_1) et connectée au dispositif de manière amovible

2. Dispositif selon la revendication 1, dans lequel la mémoire (37) est portée par un circuit électronique (36) de type carte SIM ou UICC, le dispositif comprenant un connecteur (38) pour accueillir le circuit électronique (36).

3. Dispositif selon la revendication 1 ou 2, dans lequel dans lequel le microprocesseur (32) est porté par le même circuit électronique (36) que la mémoire (37) dans laquelle est stockée la clé secrète.

4. Dispositif selon l'une des revendications1 à 3, comprenant un module d'émission sonore (34) pour fournir le mot de passe dynamique sous forme de signaux acoustiques.

5. Dispositif selon l'une des revendications 1 à 4, comprenant un afficheur (14) pour l'affichage du mot de passe dynamique.

6. Dispositif selon l'une des revendications 1 à 5, comprenant un module d'émission radiofréquences (42) pour émettre un signal radiofréquences représentatif du mot de passe dynamique.

7. Dispositif selon l'une des revendications 1 à 6, comportant une connectique (40) de type USB et pouvant être connecté sur un appareil équipé d'un port de type USB.

8. Dispositif selon la revendication 7, comprenant une batterie (30) rechargeable, la batterie étant rechargée lorsque le dispositif est connecté via le port USB.

9. Dispositif selon l'une des revendications 1 à 8, dans laquelle la mémoire (37) dans laquelle est stockée la clé secrète permet de stocker des informations complémentaires.

10. Dispositif selon l'une des revendications précédentes, dans lequel le calcul du mot de passe dynamique prend en argument la valeur d'un compteur incrémenté à chaque nouveau calcul, et/ou dépend du temps.

11. Dispositif selon l'une des revendications précédentes, dans lequel le mot de passe dynamique est simultanément fourni par le dispositif (10) via au moins deux des moyens de communication disponibles.

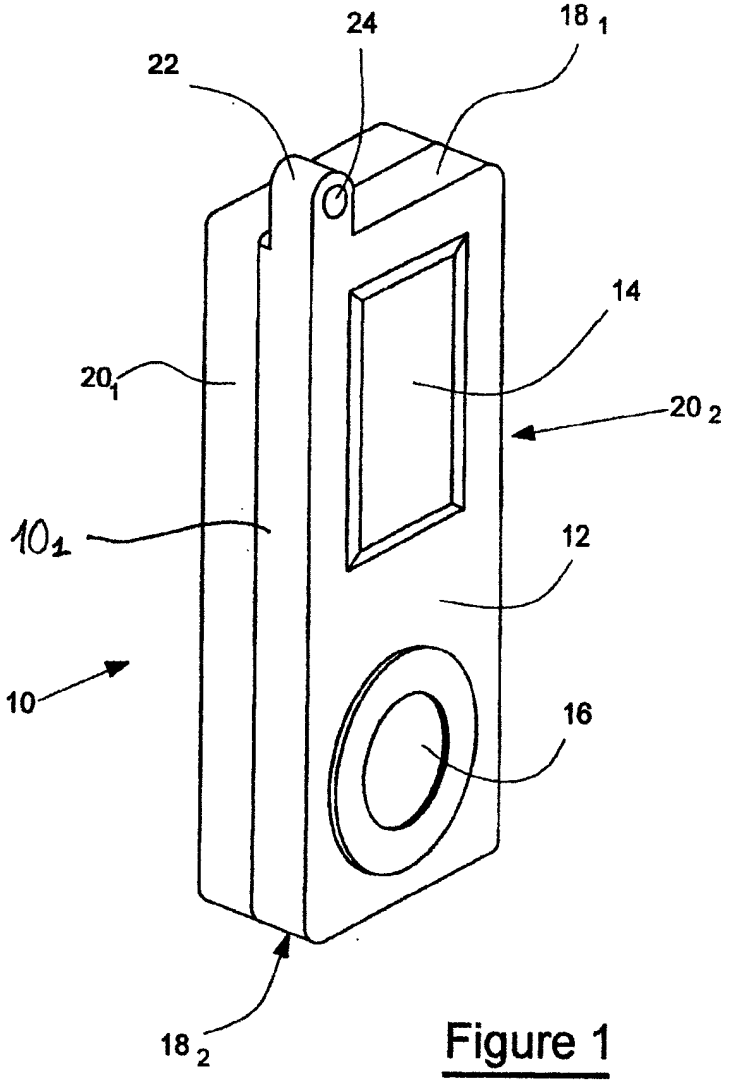

Figure 1

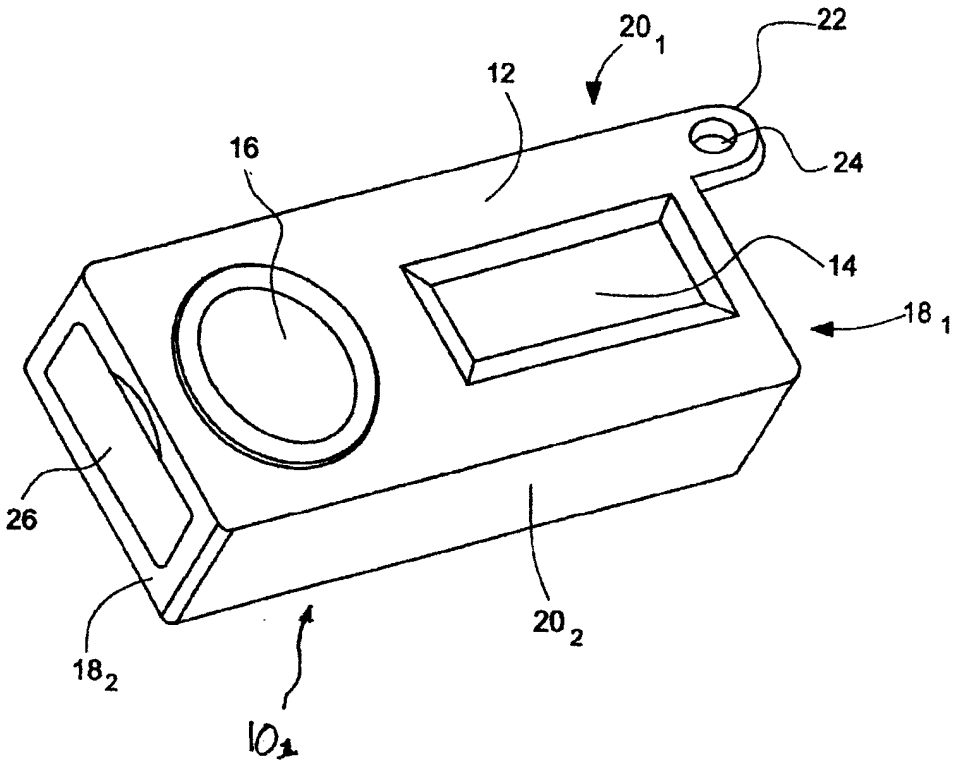

Figure 2

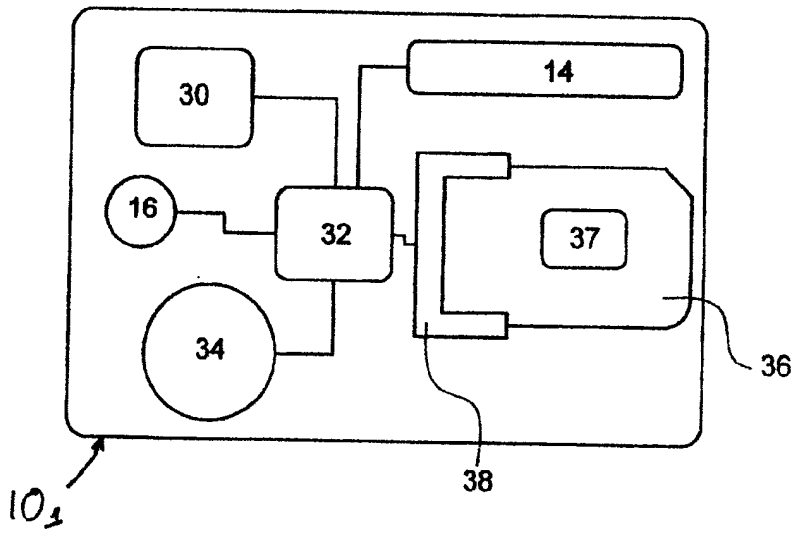

Figure 3

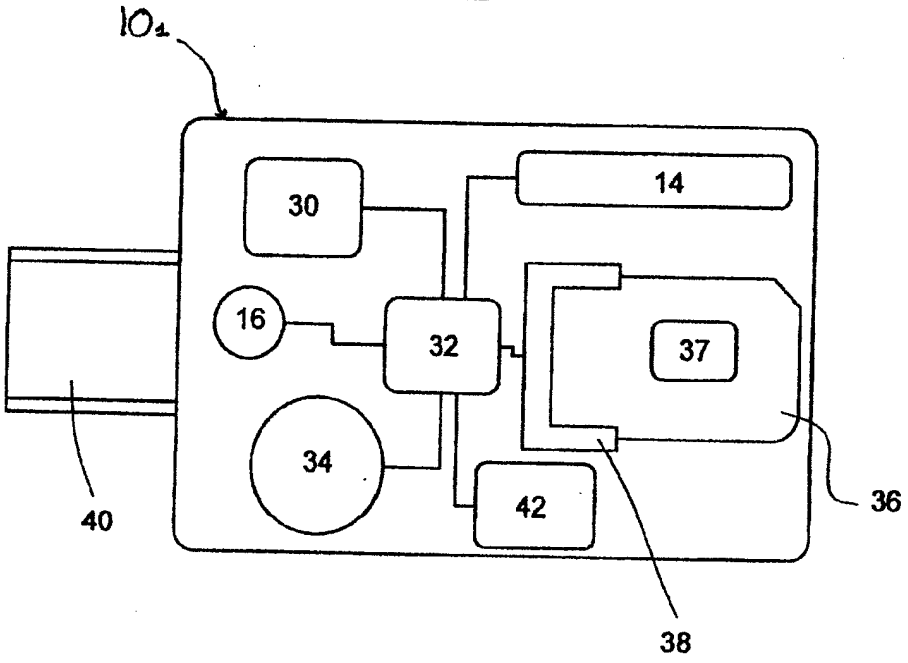

Figure 4