economie

UITVINDINGSOCTROOI

KONINKRIJK BELGIE

FOD ECONOMIE, K.M.O.,

MIDDENSTAND & ENERGIE

PUBLICATIENUMMER : 1016521A6

INDIENINGSNUMMER : 2005/0230

Internat. klassif. : G07C

Datum van verlening : 05 December 2006

De Minister van Economie,

Gelet op de wet van 28 Maart 1984 op de uitvindingsoctrooien inzonderheid artikel 22;
Gelet op het Koninklijk Besluit van 2 December 1986, betreffende het aanvragen, verlenen en in stand houden van uitvindingsoctrooien, inzonderheid artikel 28;

Gelet op het proces-verbaal opgesteld door de Dienst voor Intellectuele Eigendom op 09 Mei 2005 te 23u05

BESLUIT :

ARTIKEL 1.- Er wordt toegekend aan : LAUREYSSENS Dirk
Grote Steenweg 408/19, B-2600 ANTWERPEN(BELGIË)

een uitvindingsoctrooi voor de duur van 6 jaar, onder voorbehoud van de betaling van de jaartaksen voor : TOEGANGSSYSTEEM EN METHODE.

ARTIKEL 2.- Dit octrooi is toegekend zonder voorafgaand onderzoek van zijn octrooieerbaarheid, zonder waarborg voor zijn waarde of van de juistheid van de beschrijving der uitvinding en op eigen risico van de aanvrager(s).

Voor eensluidend verklaard afschrift

Brussel , 05 December 2006
BIJ SPECIALE MACHTIGING :

DRISQUE S.
Adviseur

S. DRISQUE
Adviseur

.be

Beschrijving: Toegangssysteem en methode.

Het integreren van een sluitwerk of toegangssysteem en electronica is reeds bekend doch er zijn nog een aantal technische mogelijkheden die nog niet werden gedaan.
Een belangrijke toepassing is een zeer eenvoudige en goedkope electronische sleutel die op een eenvoudige wijze kan gebruikt worden, dwz. met een simpele electronische connector, maar met een relatief complexe tot zeer complexe electronica en software. Een flash memory device (bv. een electronische identiteitskaart, een eenvoudige USB connector-geheugen) kan hiervoor gebruikt worden. Dit wordt dan een fysieke electronisch sleutel. Net zoals een gewone sleutel moet de eigenaar instaan voor het bezit ervan in de eenvoudigere versies. Bij meer complexe electronische sleutels kunnen bijkomende handelingen of gerelateerde electronica nodig zijn.
Een belangrijk voordeel is echter dat het toegangsmechanisme toelaat miljarden combinaties te bevatten of te genereren. De toegangscode(s) kunnen – afhankelijk van de complexiteit van het concept – dynamisch gewijzigd worden zodat het copieren quasi onmogelijk wordt. In het toegangsmechanisme (het slot) volstaat een eenvoudige electromagneet die een verschuifbaar element bevat, en dit kan zo gebouwd worden dat de 'eenvoudige tik tegen een cylinder-slot om het te openen' niet meer mogelijk is. Slechts na de instructie van het flash memory device wordt een electrisch veld in de electromagneet geschapen waardoor haar kern verschuift.

Het octrooi betreft een toegangssysteem en methode waarbij: enerzijds tenminste één solide state geheugen (12) met daarop relevante gegevens – dat in een aangepaste behuizing met ondersteunende componenten is geplaatst (bv. IC kaart, mobiele telefoon, USB solid state geheugen 10, flash memory card, Proton kaart, officiële identiteitskaart) - een draagbare fysieke electronische sleutel (10) vormt, en anderzijds tenminste één solide state geheugen (13) met daarop relevante gegevens en met ondersteunende componenten (bv. voeding 17, verbindingen, etc.) - waarvan tenminste één een fysieke electronisch aanstuurbare schakelaar (16) is - in een aangepaste vaste configuratie (11) – een sluitwerk (bv. slot) - is geplaatst, met elkaar verbindbaar zijn. Deze verbinding wordt gerealiseerd bv. via compatibele connectoren 14 en 15, contactoppervlak, draadloos, lichtimpulsen, netwerk. Bij de verbinding beginnen sleutel en vaste configuratie met elkaar data uit te wisselen waarbij bij een correct resultaat (toegangscode) de voormelde schakelaar geactiveerd wordt, dwz. geopend of gesloten wordt. Bij foutieve toegangscode wordt de toegang of

activatie geweigerd. Er wordt dus al dan niet tenminste één electrische implus gegeven aan de electromagneet (16) dewelke een slot opent of sluit, of dit mogelijk maakt.
De toegangscode(s) wordt hetzij: na elk gebruik en/of bij het eerste gebruik door een sleutel (10) in één of meerdere vaste configuraties (11) gegenereerd, na elk gebruik en/of bij het eerste gebruik door tenminste één vaste configuratie (11) in de sleutel (10) gegenereerd, verschaft door een relatief eenvoudige bevestiging door de software in voormelde vaste configuratie (slot 11), dwz zoals een IC card die geen pincode-invoer noodzaakt, of verschaft door een intensievere interactie tussen de relevante gegevens op de betrokken geheugens waarbij wel exacte gegevens (bv. pincode, biometrische input, voice, fysieke handeling, geluid, secundaire sleutels) worden toegevoegd. De toegangscode functioneert eventueel met private en public keys.
De voormelde sleutel(s) die samen sleutel(s) met gerelateerde vaste configuratie(s) kunnen aangeboden worden (bv. in één verpakking, kunnen eventueel ook apart via een verdeelautomaat aangekocht worden door gebruikers.

Solide state geheugens worden in zowel de sleutel(s) als de vaste configuratie(s) en kunnen geïntegreerd circuit (12, 13, 40) zijn, waardoor zij een zgn. Flash memory geheugen zijn (dat ook een controle-element bevat (bv. CPU). Zulk solide state geheugen, kan ook een ASIC zijn (traditionele halfgeleider).

Voormeld slot zal ondermeer dienstig zijn voor:

a. Sluitsystemen voor deuren, vensters en poorten,
b .Sluitsystemen en bedieningsystemen voor voertuigen, fietsen, toestellen en machines,
c. Sluitsystemen voor houders van goederen, voedsel, kleding, voorwerpen, geld, waardepapieren (31) en juwelen, zoals kasten, reiskoffers (30), lockers, rekken,
d . Hangsloten, fietssloten, rijwiel-staling (bv. aan stations),
e. Oppervlakte-begrenzers (bv. opklapbare constructie op parkingplaats achter de auto),
f. Electronische toestellen (gsm 32, etc.) waarbij de sleutel toegang kan geven.

De vaste configuratie kan bestaan uit tenminste: een slotmechanisme (16) dat zich achter of in het sluitoppervlak (18)(bv. deur, plaat, deksel, etc.) bevindt, een slotmechanisme waarvan het electronische impulssysteem – dat tenminste één beweging (bv. electromagnetisch veld wijzigt) aanstuurt in het slot - via een

compatible connector (bv. USB 15) verbindbaar is met voormelde sleutel. De vaste configuratie kan ook bestaan uit tenminste: een slotmechanisme dat zich in het sluitlichaam (bv. hangslot-lichaam, ringslot-lichaam) bevindt, een slotmechanisme waarvan het electronische impulssysteem – dat tenminste één beweging (bv. electromagnetisch veld wijzigt) aanstuurt in het slot - via een compatible connector verbindbaar is met voormelde sleutel, en een slotmechanisme dat quasi onlosmakelijk verbonden is met sluitsysteem (bv. beugel, band, ketting, klem,etc.).

Een contactoppervlak (33) van een sleutel of een ander electronisch toestel (bv. mobiele telefoon 32) kan in direct contact wordt gebracht met een contactoppervlak (33) of sensor van het slot (11) waarbij data worden uitgewisseld via effectieve vibraties (uit tril-elementen) en/of photonen (bv. laser-element), zodat bv. een deel van een mobiele telefoon tegen een slot wordt geplaatst én eventueel tegelijkertijd een bleu-tooth signaal/code wordt gegeven, zonder dat door derden via RF (radio-frequentie) de volledige toegangcode(s) kan gescand worden. Dit blijkt één van de problemen te zijn bij allerlei RF-identificatie systemen te zijn. Een GSM kan dan uitwendig of inwendig geconnecteerd worden met een sleutel. De relevante data van de sleutel worden dan hetzij direct hetzij indirect omgezet in trillingen en/of photon-impulsen die een zeer klein of enkel direct bereik hebben.

Een vaste configuratie bevat tenminste één element dat door het activeren van een magnetisch veld verschuifbaar (19) is waardoor een gewenst deel (bv. deur, deksel, klem, beugel) hetzij vergrendeld wordt, hetzij ontgrendeld wordt. Dit slot bevat dus tenminste één beweegbaar element (19).

De sleutel en vaste configuratie hebben dus connectoren die eenvoudige compatiele electronisch connecties zijn, bv. electronische kaart en kaart-lezer, USB connectie (14 en 15), Firewire connecties, etc. Compatibele connectoren kunnen hetzij regelmatig van vorm zijn (zoals een USB connectie), hetzij onregelmatig van vorm zijn (dwz. met gebogen contouren).

Bij onze vaste configuratie worden bij het aanbrengen van de verbinding (inplaatsen in connector, contact, wireless) en het verschaffen van de correcte informatie (ID, code, paswoord, etc.) instructies gegeven om een gesloten electronische en/of fysieke toegang te openen en/of te sluiten.

Zulke sleutel kan als alternatief gebruikt worden voor een pincode (bv. in betaalautomaten), of bv. als code-verschaffer voor een GSM

of computer. De sleutel wordt er ingeplaatst en quasi onmiddellijk nadien terug uitgenomen. Nieuwe GSM's en PDA's kunnen met zulke poort worden uitgerust.

Een sleutel is eventueel aansluitbaar op een losse electronische herprogrameerbaar eenheid (bv. tussenstuk) die het mogelijk maakt aan voorafgeprogrammeerde sleutels specifieke ID data toe te voegen, alsook aan de vaste configuratie, zodat een meer complexe en/of geindividualiseerde toegangscode wordt verkregen. Een sleutel (10) kan ook uitbreidbaar zijn met tenminste één bijkomende sleutel (22)(bv. aan de achterzijde 21 daarin in-, over of opschuifbaar) zodat een meer complexe toegangscode wordt gegenereerd. Een sleutel kan ook uitgerust zijn met een uniek IP-nummer.

Een dynamische sleutel kan verbonden zijn met een computer of electronische communicator (bv. mobiele telefoon) - die in netwerk-communicatie (bv. met Internet servers) tijdens en/of bij het beëindigen van een verbinding tenminste één nieuw paswoord genereert. Het genereren van een nieuwe toegangscode kan in een security protocol worden opgenomen, eventueel in het afsluitend deel van protocol.

De toegangscode kan ondermeer gebaseerd zijn op combinaties en/of geometrische configuraties en posities van Catalan numbers waardoor private en public keys worden verkregen. Catalan numbers of hun posities kunnen dan ook deels of geheel vervangen worden door bv. hexadecimale getallen.
Een toegangscode kan initieel gecreëerd worden door data in de sleutel (10)(zgn. Actieve sleutel), en de relevante electronische delen van de vaste configuratie (11) initieel passief zijn (zgn. Slaaf slot). Omgekeerd kan de toegangscode ook initieel gecreëerd wordt vanuit data van de vaste configuratie (11), en de sleutel (10) initieel passief is (zgn. Passieve sleutel of slaaf sleutel). Combinatie van beiden is natuurlijk ook mogelijk.
Sleutel en vaste configuratie kunnen elk uitgerust zijn met tenminste één voedingsbron (bv. batterij, zonnecel 17, etc.).

Tussen sleutel en vaste configuratie kan de toegangscode(s) continu gelden of slechts voor een bepaalde tijdsperiode (bv. twee maanden, enkel tussen 8:00 en 19:00).
De vaste configuratie (11) kan eventueel via een remote wireless systeem een central (computer) systeem informeren over haar status, ID van de gebruikte sleutel(s), het tijdstip van gebruik, duur van het gebruik, poging van misbruik (alarm), ...etc.

Een verdeelautomaat bevat tenminste: een intern aanvoersysteem voor voormelde sleutels, een betaalsysteem (bv. kredietkaart, Proton type, etc), een openingsysteem om de sleutel uit de automaat te nemen, en eventueel: een fysiek of een touch-screen klavier (bv. voor het ingeven van persoonlijke gegevens of paswoorden, ingave van het aantal identieke sleutels, type van sleutel, bestellen van een dubbele combinatie-sleutel, etc.), een electronisch systeem dat gegeneerde data in de de relevante delen van de sleutel plaatst, een data input systeem (bv. reeds bestaande sleutel, officiële ID kaart, één of meerdere biometrische sensoren of één of meerdere acoustische sensoren (om voice te registreren). Dergelijke verdeelautomaat kan zowel voor sleutels en specifieke sluitsystemen (bv. alarmsystemen, hangsloten, fietssloten, etc.) aanbieden.

Diverse alarmsystemen kunnen geactiveerd en gedesactiveerd worden via voormelde sleutel(s).

Een sleutel kan ook dienstig zijn voor het anoniem identificeren van een geautoriseerde gebruiker op Internet en andere netwerken. Anonimiteit wordt gewenst door de meeste Internetgebruikers. Bij het inloggen kan de ontvangende server via de sleutel – die bv. maar even door de gebruiker in de gerelateerde poort wordt gestoken – weten dat de inlogger de gebruiker/bezitter van de originele sleutel is. Dit voorkomt dat via Spyware toegangscode van de computer wordt gehaald, zoals momenteel regelmatig gebeurt. Het gebruik van dergelijke sleutel maakt zeer ingewikkelde toegangscodes mogelijk, en is gebruiksvriendelijk. Via de software tussen computer en sleutel kan voorzien zijn dat de poort quasi onmiddellijk wordt gesloten na het geven van de identificatie code. Een aparte firewall kan hiervan deeluitmaken. Zulke sleutel kan ook dienstig zijn voor het identificeren van een geautoriseerde gebruiker op Internet en andere netwerken en het opstarten van een beveiligde communicatie (shttp).
Op deze sleutel kan tenminste één organiserende server op Internet en/of op een ander netwerk (bv. intranet) een toegangscode genereren op de aangesloten sleutel van de gebruiker.

Een sleutel kan als algemene sleutelhanger kan gebruikt worden (bv. met tenminste één opening), en eventueel aan een sleutelring hangen.
De sleutel kan in een special compatiebele ruimte van een mobiele telefoon (32) of andere electronisch apparaat geplaatst worden, en daarbij hetzij actief zijn – en extra electronische storage ruimte

geven (bv. voor mp3-files) - , hetzij passief zijn (enkel opgeslagen worden voor later gebruik). De GSM wordt dan een sleutel houder. De sleutel voor het activeren kan dan tegelijkertijd de sleutel zijn voor het activeren van diverse electronische apparaten (34), als de sleutel voor de voordeur als de sleutel voor valiezen. Dit is dus uitermate gebruiksvriendelijk. En zulke sleutel kan ook te gebruiken zijn als een instructie-eenheid voor diverse soorten 'prefered settings', bv. een auto-zetel, machine, instrument, etc.

Een speciaal geïntegreerd circuit (40) is mogelijk als extra beveiliging, namelijk dat modulair is. Meer bepaald een IC waarvan tenminste één module (42) zich in de bovenvermelde sleutel bevindt en tenminste één module (41) zich in de vaste configuratie bevindt, zodat slechts bij een effectieve connectie tussen sleutel en vaste configuratie de modules effectief een geheel vormen en kan werken. Dus beiden moeten met elkaar verbonden zijn om de gewenste electronische verwerking mogelijk te maken. Diverse soorten en concepten van modules zijn mogelijk zodat men aan het slot niet kan vaststellen welke corresponderende module in de sleutel noodzakelijk is, en bovendien moet ook een toegangscode verschaft worden. Het is dus een methode en technologie waarbij twee of meerdere delen van een geïntegreerd circuit worden ingewerkt in aparte met elkaar verbindbare electronische systemen, waarbij het geïntegreerd circuit werkt van het moment dat de electronische systemen met elkaar verbonden worden, bv. als de juiste sleutel met de juiste module in de juiste vaste configuratie met de juiste module wordt geplaatst. De beveiliging is bijgevolg dubbel, zowel via de toegangscode maar ook via de hardware in zowel sleutel als slot. Er is nog een erg interessante toepassing, namelijk een automatisch alarm dat geactiveerd wordt indien een foutieve sleutel-IC-module wordt gebruikt. Dus louter de poging reeds geeft een alarm-signaal.
Deze methode en technologie kan ook gebruikt worden voor servers die dan ook uitgerust worden met gesplitste geïntgreerde circuits (41 en 42) waarbij over het netwerk de werkzaamheden van één of meerdere IC's plaats hebben. De mogelijke vertraging weegt niet op tegen de uitzonderlijke veiligheid. Men kan hier spreken van een remote IC of network IC. In een groter netwerk kunnen met network IC's uitgerustte computers aldus switchen afhankelijk van de connecterende servers.

De methode en technologie ivm sleutels kan ook gebruikt worden tegen e-mail-spam. Dan wordt een externe (in computer poort te steken) sleutel gebruikt voor het generen van unieke e-mail tags die aan elke e-mail correspondent (per e-mail adres) een public-key-tag toekent dewelke door de correspondent moet gebruikt

worden (bv. als attachment, als numeriek e-mail adres) in zijn communicatie met die betrokkene, zodat de betreffende e-mail automatisch – na controle van de correspondentie tussen e-mail adres met de public-key – als 'aanvaardbaar' (niet-spam) wordt beoordeeld en eventueel gestockeerd in een speciale account van het e-mail programma. Dergelijk tag is dan niet overdraagbaar aan anderen en maakt e-mail communicatie beveiligd.
Deze methode en technologie is ook toepasselijk voor telefonie en multi-media communicatie (bv. ontvangen van SMS, MMS) door het connecteren van een telefoon (bv. mobiele telefoon, PDA) met dergelijke externe sleutel.
Deze methode en technologie kan gebruikt worden door een service provider (bv. SMPT – IMAP server) op de servers als pre-filter, eventueel op instructie van een sleutel, zoals beschreven in conclusie 1, van haar klant.

Verder in relatie met de sleutels wordt een methode en technologie voorzien waarbij in een geïntegreerd circuit (40), zoals beschreven in conclusie 2, een resonantiekring (43) is verwerkt die bij foutieve frequenties verbroken wordt. Hierdoor wordt het IC vernietigd op een essentiële wijze. Een alternatieve methode en technologie is die waarbij een separate IC module(s) in een sleutel(s) zit, waardoor bij het inbrengen van de sleutel, het volledige geïntegreerd circuit (40), zoals beschreven in conclusie 2, vervolledigd wordt en aldus de werking van een electronisch toestel mogelijk maakt, bv. te gebruiken voor computers, robots, machines, mobiele telefoons, PDA's, ontstekingsmechanisme auto, etc.

Conclusies:

1. Toegangssysteem en methode waarbij:
   a. enerzijds tenminste één solide state geheugen (12) met daarop relevante gegevens – dat in een aangepaste behuizing met ondersteunende componenten is geplaatst (bv. IC kaart, mobiele telefoon, USB solid state geheugen 10, flash memory card, Proton kaart, officiële identiteitskaart) - een draagbare fysieke electronische sleutel (10) vormt,
   b. en anderzijds tenminste één solide state geheugen (13) met daarop relevante gegevens en met ondersteunende componenten (bv. voeding 17, verbindingen, etc.) - waarvan tenminste één een fysieke electronisch aanstuurbare schakelaar (16) is - in een aangepaste vaste configuratie (11) – een sluitwerk (bv. slot) - is geplaatst,

   met elkaar verbindbaar zijn (bv. via compatibele connectoren 14 en 15, contactoppervlak, draadloos, lichtimpulsen, netwerk) en in dat geval met elkaar data uitwisselen waarbij bij een correct resultaat (toegangscode) de voormelde schakelaar geactiveerd wordt, dwz. geopend of gesloten wordt waardoor al dan niet tenminste één electrische implus wordt gegeven aan een electromagneet (16) dewelke een slot opent of sluit, of dit mogelijk maakt,
   en de toegangscode(s) hetzij:
   c. na elk gebruik en/of bij het eerste gebruik door een sleutel (10) in één of meerdere vaste configuraties (11) wordt gegenereerd,
   d. na elk gebruik en/of bij het eerste gebruik door tenminste één vaste configuratie (11) in de sleutel (10) wordt gegenereerd,
   e. verschaft wordt door een relatief eenvoudige bevestiging door de software in voormelde vaste configuratie (slot 11), dwz zoals een IC card die geen pincode-invoer noodzaakt,
   f. verschaft wordt door een intensivere interactie tussen de relevante gegevens op de betrokken geheugens waarbij wel exacte gegevens (bv. pincode, biometrische input, voice, fysieke handeling, geluid, secundaire sleutels) worden toegevoegd,
   g. functioneert met private en public keys,

   en waarbij voormelde sleutel(s) – naast het samen aanbieden van specifieke sleutel(s) met gerelateerde vaste configuratie(s) – sleutels (10) eventueel via een verdeelautomaat kunnen aangekocht worden door gebruikers;

2. Solide state geheugen, zoals beschreven in conclusie 1, dat een geïntegreerd circuit (12, 13, 40) is;

3. Solide state geheugen, zoals beschreven in conclusie 1, dat een ASIC is;

4. Slot, zoals beschreven in conclusie 1, ondermeer dienstig voor:

   a. Sluitsystemen voor deuren, vensters en poorten,
   b .Sluitsystemen en bedieningsystemen voor voertuigen, fietsen, toestellen en machines,
   c. Sluitsystemen voor houders van goederen, voedsel, kleding, voorwerpen, geld, waardepapieren (31) en juwelen, zoals kasten, reiskoffers (30), lockers, rekken,
   d. Hangsloten, fietssloten, rijwiel-staling,
   e. Oppervlakte-begrenzers (bv. opklapbare constructie op parkingplaats),
   f. Electronische toestellen (gsm, etc.);

5. Vaste configuratie, zoals beschreven in conclusie 1, bestaande uit tenminste:

   a. een slotmechanisme (16) dat zich achter of in het sluitoppervlak (18)(bv. deur, plaat, deksel, etc.) bevindt,
   b .slotmechanisme waarvan het electronische impulssysteem – dat tenminste één beweging (bv. electromagnetisch veld wijzigt) aanstuurt in het slot - via een compatible connector (bv. USB 15) verbindbaar is met voormelde sleutel;

6. Vaste configuratie, zoals beschreven in conclusie 1, bestaande uit tenminste:

   a. een slotmechanisme dat zich in het sluitlichaam (bv. hangslot-lichaam, ringslot-lichaam) bevindt,
   b .slotmechanisme waarvan het electronische impulssysteem – dat tenminste één beweging (bv. electromagnetisch veld wijzigt) aanstuurt in het slot - via een compatible connector verbindbaar is met voormelde sleutel,
   c. slotmechanisme dat quasi onlosmakelijk verbonden is met sluitsysteem (bv. beugel, band, ketting, klem,etc.);

7. Contactoppervlak (33), zoals beschreven in conclusie 1, van een sleutel of een ander electronisch toestel (bv. mobiele telefoon 32) dat in direct contact wordt gebracht met een contactoppervlak (33) of sensor van het slot (11) waarbij data worden uitgewisseld via effectieve vibraties (uit tril-elementen) en/of photonen (bv. laser-element), zodat bv. een deel van een mobiele telefoon tegen een slot wordt geplaatst én eventueel tegelijkertijd een bleu-tooth signaal/code wordt gegeven, zonder dat door derden via RF (radio-frequentie) de volledige toegangcode(s) kan gescand worden;

8. Vaste configuratie, zoals beschreven in conclusie 1, bevattend tenminste één element dat door het activeren van een magnetisch veld verschuifbaar (19) is waardoor een gewenst deel (bv. deur, deksel, klem, beugel) hetzij vergrendeld wordt, hetzij ontgrendeld wordt;

9. Slot, zoals beschreven in conclusie 1, bevattend tenminste één beweegbaar element (19);

10. Sleutel en vaste configuratie, zoals beschreven in conclusie 1, waarvan de connectoren eenvoudige compatiele electronisch connectie zijn, bv. electronische kaart en kaart-lezer, USB connectie (14 en 15), Firewire connecties, etc.;

11. Compatibele connectoren, zoals beschreven in conclusie 1, die hetzij regelmatig van vorm zijn, hetzij onregelmatig van vorm zijn;

12. Vaste configuratie, zoals beschreven in conclusie 1, die bij het aanbrengen van de verbinding (inplaatsen in connector, contact, wireless) en het verschaffen van de correcte informatie (ID, code, paswoord, etc.) instructies geeft om een gesloten electronische en/of fysieke toegang te openen en/of te sluiten;

13. Sleutel, zoals beschreven in conclusie 1, die als alternatief kan gebruikt worden voor een pincode (bv. in betaalautomaten);

14. Sleutel, zoals beschreven in conclusie 1, dewelke aansluitbaar is op een losse electronische herprogrameerbaar eenheid (bv. tussenstuk) die het mogelijk maakt aan voorafgeprogrammeerde sleutels specifieke ID data toe te voegen, alsook aan de vaste configuratie, zodat een meer complexe en/of geindividualiseerde toegangscode wordt verkregen;

15. Sleutel (10), zoals beschreven in conclusie 1, die uitbreidbaar is met tenminste één bijkomende sleutel (22)(bv. aan de achterzijde 21 daarin in-, over of opschuifbaar) zodat een meer complexe toegangscode wordt gegenereerd;

16. Sleutel, zoals beschreven in conclusie 1, die is uitgerust met een uniek IP-nummer;

17. Sleutel, zoals beschreven in conclusie 1, - verbonden met de computer of electronische communicator (bv. mobiele telefoon) - die in netwerk-communicatie (bv. met Internet servers) tijdens en/of bij het beëindigen van een verbinding tenminste één nieuw paswoord genereert;

18. Toegangscode, zoals beschreven in conclusie 1, die ondermeer gebaseerd is op combinaties en/of geometrische configuraties en posities van Catalan numbers waardoor private en public keys worden verkregen;

19. Toegangscode, zoals beschreven in conclusie 1, welke initieel gecreëerd wordt door data in de sleutel (10)(zgn. Actieve sleutel), en de relevante electronische delen van de vaste configuratie (11) initieel passief zijn (zgn. Slaaf slot);

20. Toegangscode, zoals beschreven in conclusie 1, welke initieel gecreëerd wordt data van de vaste configuratie (11), en de sleutel (10) initieel passief is (zgn. Passieve sleutel of slaaf sleutel);

21. Sleutel en vaste configuratie, zoals beschreven in conclusie 1, die elk uitgerust kunnen zijn met tenminste één voedingsbron (bv. batterij, zonnecel 17, etc.);

22. Sleutel en vaste configuratie, zoals beschreven in conclusie 1, waarvan de toegangscode slechts voor een bepaalde tijdsperiode geldt (bv. twee maanden, enkel tussen 8:00 en 19:00);

23. Vaste configuratie (11), zoals beschreven in conclusie 1, die via een remote wireless systeem een central systeem informeert over haar status, ID van de gebruikte sleutel, het tijdstip van gebruik, duur van het gebruik, poging van misbruik (alarm), etc.;

24. Verdeelautomaat, zoals beschreven in conclusie 1, bevattend tenminste:

a. een intern aanvoersysteem voor voormelde sleutels,
b. een betaalsysteem (bv. kredietkaart, Proton type, etc),
c. een openingsysteem om de sleutel uit de automaat te nemen,
d. en eventueel:
    i. een fysiek of een touch-screen klavier (bv. voor het ingeven van persoonlijke gegevens of paswoorden, ingave van het aantal identieke sleutels, type van sleutel, bestellen van een dubbele combinatie-sleutel, etc.),
    ii. een electronisch systeem dat gegeneerde data in de de relevante delen van de sleutel plaatst,
    iii. een data input systeem (bv. reeds bestaande sleutel, officiële ID kaart,
    iv. één of meerdere biometrische sensoren,
    v. één of meerdere acoustische sensoren;

25. Verdeelautomaat, zoals beschreven in conclusie 1, voor sleutels en specifieke sluitsystemen (bv. alarmsystemen, hangsloten, fietssloten, etc.);

26. Alarmsysteem, zoals beschreven in conclusie 1, dat geactiveerd en gedesactiveerd kan worden via voormelde sleutel(s);

27. Sleutel, zoals beschreven in conclusie 1, dienstig voor het anoniem identificeren van een geautoriseerde gebruiker op Internet en andere netwerken;

28. Sleutel, zoals beschreven in conclusie 1, dienstig voor het identificeren van een geautoriseerde gebruiker op Internet en andere netwerken en het opstarten van een beveiligde communicatie;

29. Sleutel, zoals beschreven in conclusie 1, waarop tenminste één organiserende server op Internet en/of op een ander netwerk (bv. intranet) een toegangscode genereert op de aangesloten sleutel van een gebruiker;

30. Sleutel, zoals beschreven in conclusie 1, die als algemene sleutelhanger kan gebruikt worden (bv. met tenminste één opening);

31. Sleutel, zoals beschreven in conclusie 1, die in een special compatiebele ruimte van een mobiele telefoon (32) of andere electronisch apparaat kan geplaatst worden, en daarbij hetzij

actief is – en extra electronische storage ruimte kan geven (bv. voor mp3-files - , hetzij passief is (enkel opgeslagen wordt);

32. Sleutel, zoals beschreven in conclusie 1, te gebruiken als een instructie-eenheid voor diverse soorten 'prefered settings', bv. een auto-zetel, een machine;

33. Geïntegreerd circuit (40), zoals beschreven in conclusie 2, dat modulair is, meer bepaald waarvan tenminste één module (42) zich in de bovenvermelde sleutel bevindt en tenminste één module (41) zich in de vaste configuratie bevindt, zodat slechts bij een effectieve connectie tussen sleutel en vaste configuratie de modules effectief een geheel vormen en kan werken;

34. Methode en technologie waarbij twee of meerdere delen van een geïntegreerd circuit, zoals beschreven in conclusie 2, worden ingewerkt in aparte met elkaar verbindbare electronische systemen, waarbij het geïntegreerd circuit werkt van het moment dat de electronische systemen met elkaar verbonden worden, bv. als de juiste sleutel in de juiste configuratie wordt geplaatst, en eventueel bij het plaatsen van een verkeerde (niet-geautoriseerde) sleutel automatisch een alarm-module geactiveerd wordt;

35. Methode en technologie, zoals beschreven in conclusie 34, waarbij servers uitgerust worden met gesplitste geïntgreerde circuits (41 en 42);

36. Methode en technologie waarbij een externe sleutel, zoals beschreven in conclusie 1, gebruikt wordt voor het generen van unieke e-mail tags die aan elke e-mail correspondent (per e-mail adres) een public-key-tag toekent dewelke moet gebruikt worden (bv. als attachment, als numeriek e-mail adres) door de correspondent in zijn communicatie met die betrokkene, zodat de betreffende e-mail automatisch – na controle van de correspondentie tussen e-mail adres met de public-key – als 'aanvaardbaar' (niet-spam) wordt beoordeeld en eventueel gestockeerd;

37. Methode en technologie, zoals beschreven in conclusie 36, dat ook toepasselijk is voor telefonie en multi-media communicatie (bv. ontvangen van SMS, MMS) door het connecteren van een telefoon (bv. mobiele telefoon, PDA) met dergelijke externe sleutel;

38. Methode en technologie, zoals beschreven in conclusie 36, te gebruiken door de service provider (bv. SMPT – IMAP server) op haar servers als pre-filter, eventueel op instructie van een sleutel, zoals beschreven in conclusie 1, van haar klant;

39. Methode en technologie waarbij in een geïntegreerd circuit (40), zoals beschreven in conclusie 2, een resonantiekring (43) is verwerkt die bij foutieve frequenties verbroken wordt en aldus het IC verbreekt;

40. Methode en technologie waarbij een separate IC module(s) in een sleutel(s) het volledige geïntegreerd circuit (40), zoals beschreven in conclusie 2, vervolledigt en aldus de werking van een electronisch toestel mogelijk maakt, bv. computer, robot, machine, mobiele telefoon, ontstekingsmechanisme auto, etc.

Fig. 1

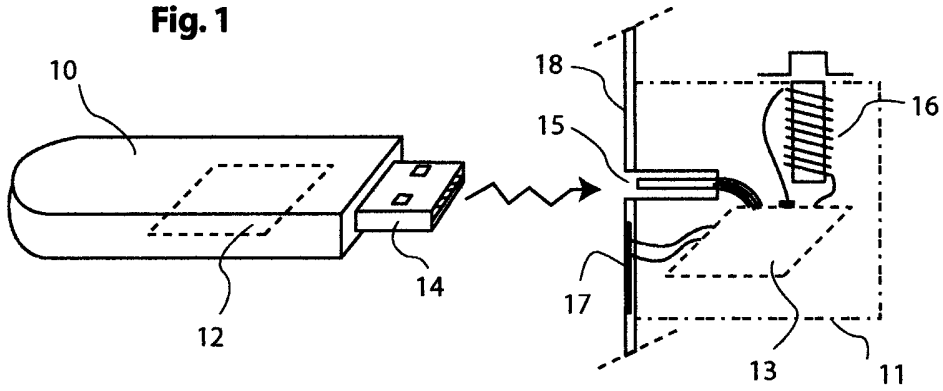


Fig. 2

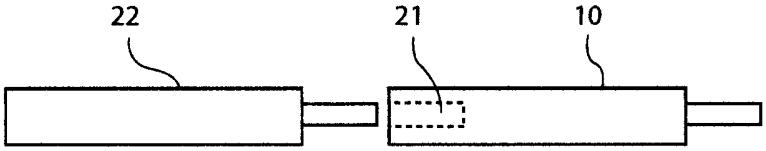


Fig. 3

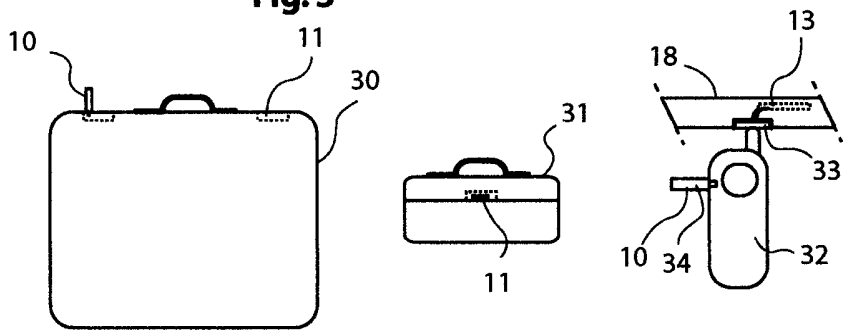
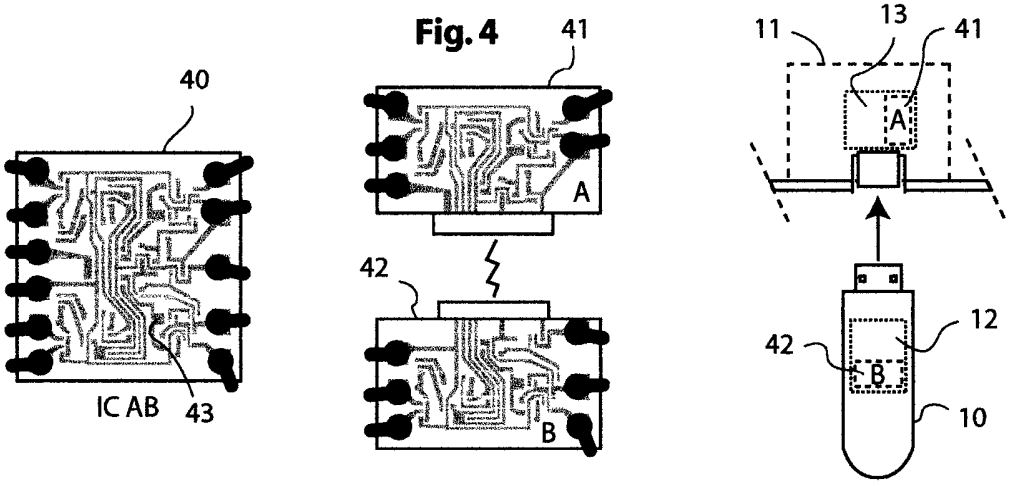


Fig. 4



Uittreksel: Toegangssysteem en methode.

Een eenvoudige electronische sleutel met simpele electronische connector heeft een relatief complexe e electronica en software. Een flash memory device (bv. electronische identiteitskaart, USB connector-geheugen) wordt gebruikt. Copieren is quasi onmogelijk. Een electrisch veld wordt in een electromagneet geschapen waardoor haar kern verschuift. De sleutel kan actief of passief zijn. Sleutels kunnen via een verdeelautomaat aangekocht worden. Sleutels als alternatief te gebruiken voor pincodes. Een speciaal modulair geïntegreerd circuit is mogelijk als extra beveiliging, een module in de sleutel en een module in het slot, beiden moeten met elkaar verbonden zijn om electronische verwerking mogelijk te maken, bij foutieve sleutel gaat een alarm. Servers en andere toestellen met gesplitste IC's zijn mogelijk, alsook geïntegreerd circuits met verbreekbare resonantiekring(en).