(19) DANMARK (10) DK 2002 00630 L

(12) PATENTANSØGNING

Patent- og
Varemærkestyrelsen

(51) Int.Cl[7].: G 06 K 9/00

(21) Patentansøgning nr: PA 2002 00630

(22) Indleveringsdag: 2002-04-27

(24) Løbedag: 2002-03-22

(41) Alm. tilgængelig: 2003-01-09

(86) International ansøgning nr: PCT/SG02/00047

(86) International indleveringsdag: 2002-03-22

(85) Videreførelsesdag: 2002-04-27

(30) Prioritet: 2001-06-28 WO PCT/SG01/00134

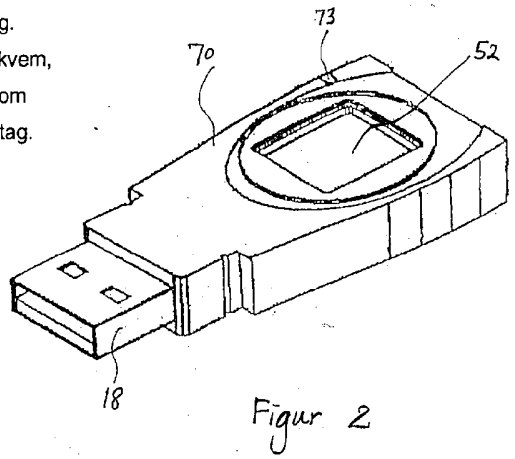
(71) Ansøger: Trek 2000 International Ltd., 30 Loyang Way #07-13/14/15, Loyang Industrial Estate, Singapore 508769, Singapore

(72) Opfinder: Teng Pin Poo, Apt Blk 44 Bedok South Road #11-763, Singapore 460044, Singapore
Lay Chuan Lim, Apt Blk 322 Bukit Batok Street #03-04, Singapore 650322, Singapore

(74) Fuldmægtig: Awapatent A/S, Teglholm Alle 13, 4. sal, 2450 København SV, Danmark

(54) Benævnelse: Bærbar enhed omfattende biometrisk baserede verificeringsegenskaber

(57) Sammendrag:
Apparat og metode til implementering af biometrisk baseret verificering. I en foretrukket udførelsesform er foreliggende opfindelse udført i en bærbar enhed. Særligt, i en udførelsesform, inkluderer den bærbare enhed en mikroprocessor, en ikke-flygtig hukommelse koblet dertil, og et biometrisk baseret verificeringsmodul styret af mikroprocessoren. Fortrinsvis er den anvendte biometriske teknologi fingeraftryksverificeringsteknologi. Verificeringsmodulet kan registrere et fingeraftryk ved første brug af den bærbare enhed og gemme en indkodet version af fingeraftrykket i den ikke-flygtige hukommelse. Derefter kan verificeringsmodulet læse en brugers fingeraftryk og på pålidelig vis afgøre, hvorvidt fingeraftrykket matcher det registrerede fingeraftryk gemt i den ikke-flygtige hukommelse. Hvis et match konstateres, gives adgang til information i den ikke-flygtige hukommelse til personen; ellers nægtes adgang. Udførelsesformer af foreliggende opfindelse tilvejebringer således en yderst bekvem, sikker og pålidelig metode og system til brugerverificering og adgangskontrol, som ikke har kunnet opnås via den kendte tekniks passwordbaserede verificeringstiltag.



Figur 2

Patentkrav

1. Bærbar enhed omfattende:

en mikroprocessor;

en ikke-flygtig hukommelse koblet til mikroprocessoren; og

et biometrisk baseret verificeringsmodul koblet til og styret af mikroprocessoren, hvor adgang til den ikke-flygtige hukommelse gives til en bruger, forudsat at det biometrisk baserede verificeringsmodul verificerer brugerens identitet, og hvor adgang til den ikke-flygtige hukommelse ellers nægtes brugeren.

2. Bærbar enhed ifølge krav 1, hvor det biometrisk baserede verificeringsmodul er et fingeraftryksverificeringsmodul.

3. Bærbar enhed ifølge krav 2, hvor fingeraftryksverificeringsmodulet omfatter et fingeraftrykssensorelement.

4. Bærbar enhed ifølge krav 3, hvor sensorelementet kan rotereunder en detekteringsoperation, for at bringe på hinanden følgende dele af brugerens finger i rullende kontakt med sensoren og derved registrere på hinanden følgende dele af brugerens fingeraftryk.

5. Bærbar enhed ifølge krav 3 eller 4, hvor fingeraftryksverificeringsmodulet omfatter et låg, monteret til bevægelse mellem en første position, hvor sensorelementet dækkes, og en anden position, hvor sensoren afdækkes.

6. Bærbar enhed ifølge et hvilket som helst af de foregående krav, yderligere omfattende en universel seriel bus-konnektor (USB-konnektor), som kan kobles med en anden USB-kompatibel enhed.

7. Bærbar enhed ifølge et hvilket som helst af de foregående krav, hvor det biometrisk baserede verificeringsmodul omfatter en biometrisk sensor monteret på en overflade på den bærbare enhed.

8. Bærbar enhed ifølge et hvilket som helst af de foregående krav, hvor den ikke-flygtige hukommelse omfatter flash-hukommelse.

9. Bærbar enhed ifølge et hvilket som helst af de foregående krav, hvor mikroprocessoren er konfigureret til at tilvejebringe en alternativ verificeringsmekanisme, når det biometrisk baserede verificeringsmodul konstaterer verificeringsfejl.

10. Bærbar enhed omfattende:

en bus;

en mikroprocessor koblet til bussen;

en ikke-flygtig hukommelse koblet til bussen; og

et biometrisk baseret verificeringsmodul koblet til bussen, hvor det biometrisk baserede verificeringsmodul, styret af mikroprocessoren, er konfigureret til at (1) registrere en første biometrisk markør (2); lagre den første biometriske markør i den ikke-flygtige hukommelse; (3) registrere en anden biometrisk markør; og (4) konstatere om den anden biometriske markør kan verificeres sammenlignet med den første biometriske markør.

11. Bærbar enhed ifølge krav 10, hvor det biometrisk baserede verificeringsmodul er et fingeraftryksverificeringsmodul.

12. Bærbar enhed ifølge krav 10 eller 11, yderligere omfattende en universel seriel bus (USB)-kontrolenhed, der er koblet til bussen, og en USB-konnektor, der er koblet til bussen, så den bærbare enhed kan kommunikere med en værtsplatform via USB-konnektoren.

13. Bærbar enhed ifølge et hvilket som helst af kravene 10 til 12, hvor det biometrisk baserede verificeringsmodul er strukturelt integreret med den bærbare enhed i en samlet konstruktion og omfatter en biometrisk sensor placeret på en overflade på den bærbare enhed.

14. Bærbar enhed ifølge krav 13, hvor sensoren er en fingeraftrykssensor og indeholder et element, som kan rotere under en detekteringsoperation, for at bringe på hinanden følgende dele af en brugers finger i rullende kontakt med sensoren og derved registrere på hinanden følgende dele af brugerens fingeraftryk.

15. Bærbar enhed ifølge krav 13 eller 14, hvor det biometrisk baserede verificeringsmodul omfatter et låg monteret til bevægelse mellem en første position, hvor sensorelementet dækkes, og en anden position, hvor sensoren afdækkes.

16. Bærbar enhed ifølge et hvilket som helst af kravene 10 til 15, hvor den ikke-flygtige hukommelse omfatter flash-hukommelse.

17. Bærbar enhed ifølge et hvilket som helst af kravene 10 til 16, hvor det biometrisk baserede verificeringsmodul yderligere er konfigureret til at kryptere den første biometriske markør, før den første biometriske markør lagres i den ikke-flygtige hukommelse.

18. Bærbar enhed ifølge et hvilket som helst af kravene 10 til 17, hvor mikroprocessoren er konfigureret til at dirigere det biometrisk baserede verificeringsmodul til at registrere og lagre den første biometriske markør, forudsat at ingen biometrisk markør er blevet lagret i den ikke-flygtige hukommelse.

19. Bærbar enhed ifølge et hvilket som helst af kravene 10 til 18, mikroprocessoren er konfigureret til at kunne give adgang til den ikke-flygtige hukommelse, når det biometrisk baserede verificeringsmodul konstaterer en vellykket verificering.

20. Bærbar enhed ifølge et hvilket som helst af kravene 10 til 19, hvor mikroprocessoren er konfigureret til at kunne forhindre adgang til den ikke-flygtige hukommelse, når det biometrisk baserede verificeringsmodul konstaterer en mislykket verificering.

21. Bærbar enhed ifølge et hvilket som helst af kravene 10 til 20hvor mikroprocessoren er konfigureret til at kunne tilvejebringe en alternativ verificeringsmekanisme, når det biometrisk baserede verificeringsmodul konstaterer en mislykket verificering.

22. En biometrisk baseret verificeringsmetode implementeret ved brug af en bærbar enhed, hvilken metode omfatter trinene:

    (a) at registrere en første biometrisk markør fra en bruger med en biometrisk sensor installeret på den bærbare enhed;

    (b) at hente en registreret biometrisk markør fra en hukommelse i den bærbare enhed, hvor den registrerede biometriske markør blev gemt under en registreringsproces;

(c) at sammenligne den første biometriske markør med den registrerede biometriske markør; og

(d) at signalere, at verificeringen er vellykket, forudsat at et match identificeres på nævnte trin (c).

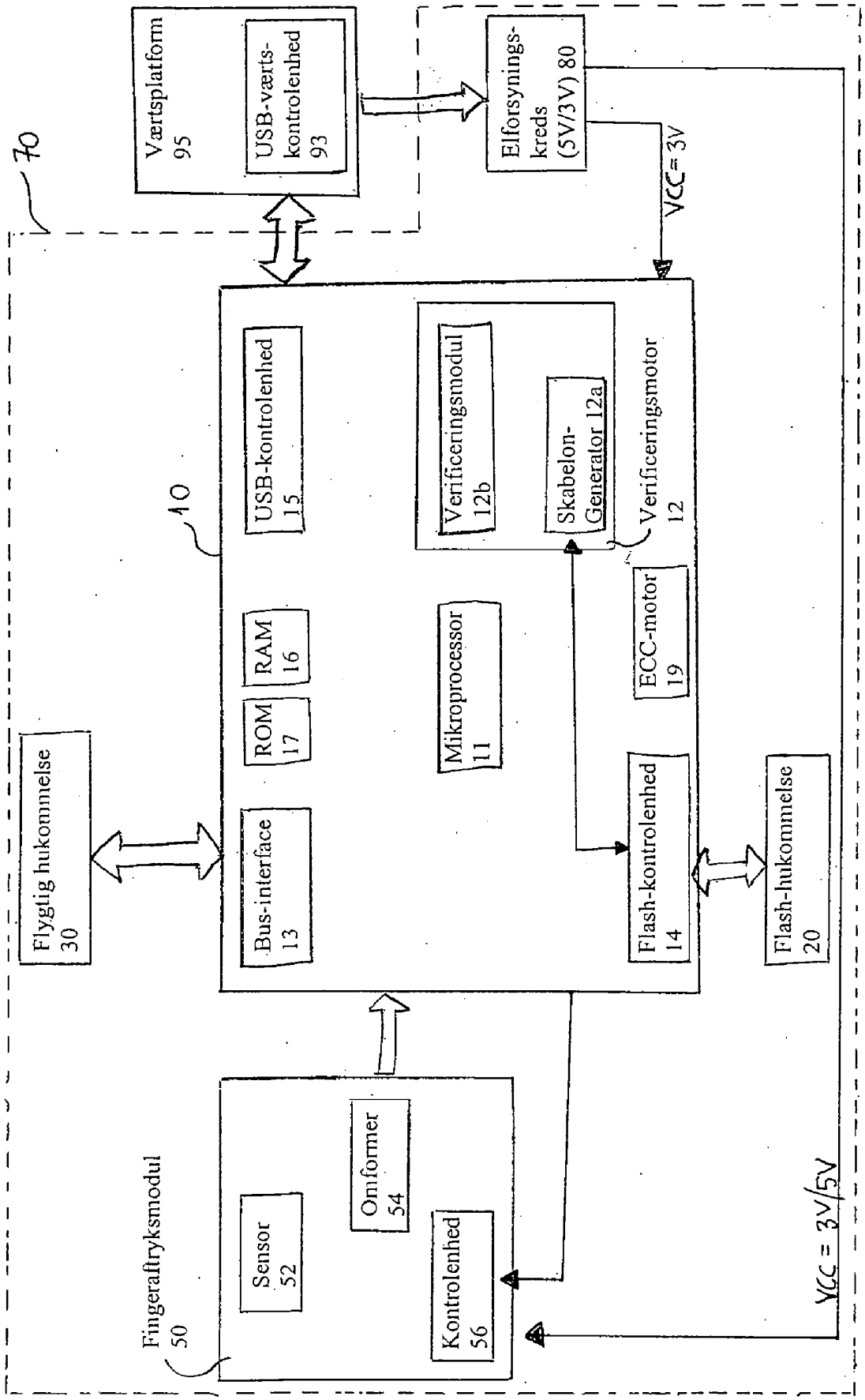
23. Biometrisk baseret verificeringsmetode som beskrevet i krav 22, hvor den registrerede biometriske markør er et fingeraftryk.

24. Biometrisk baseret verificeringsmetode ifølge krav 22 eller 23, hvor den registrerede biometriske markør er lagret i et krypteret format.

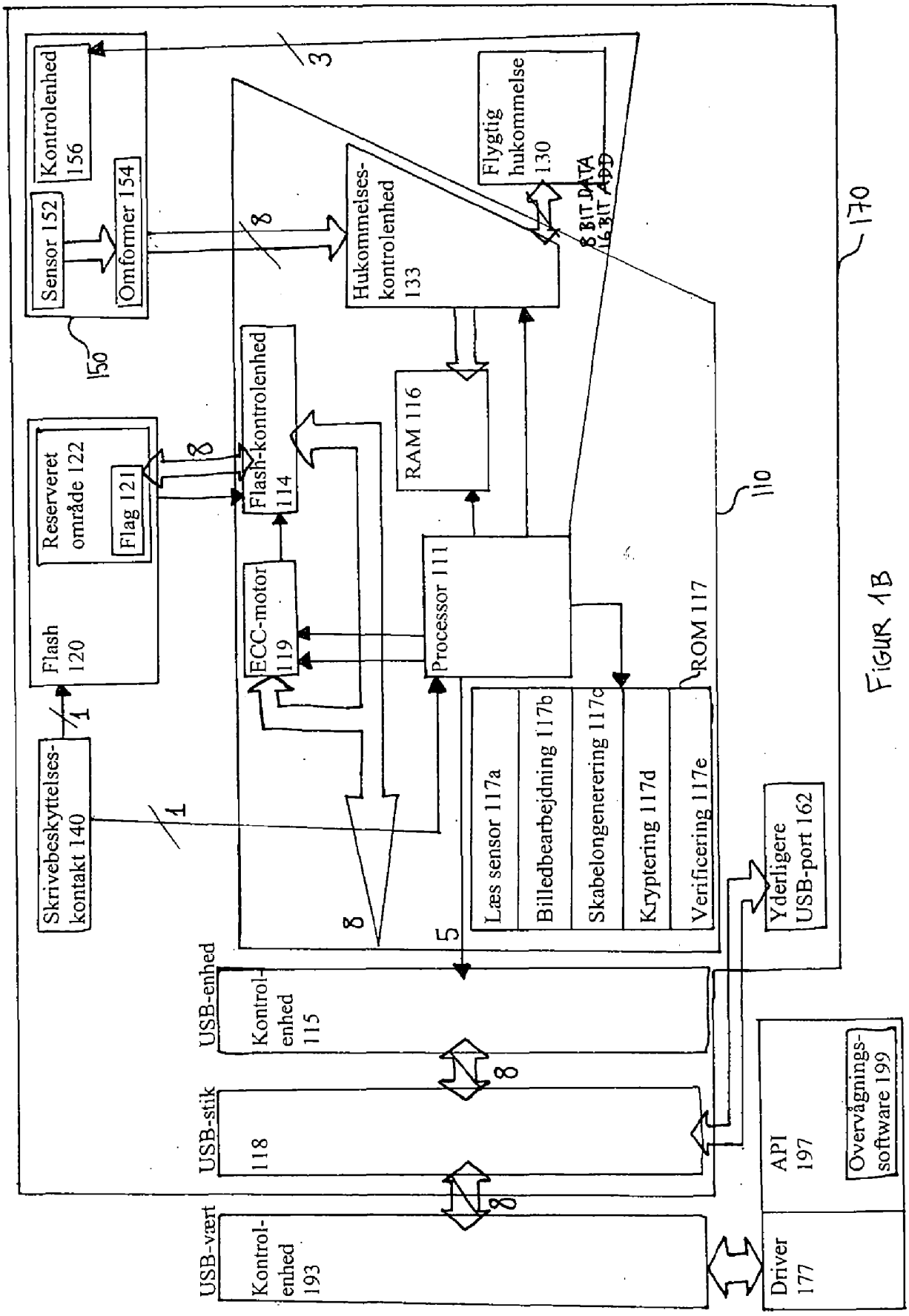
25. Biometrisk baseret verificeringsmetode ifølge et hvilket som helst af kravene 22 til 24, hvor nævnte trin (d) omfatter at give brugeren adgang til den ikke-flygtige hukommelse.

26. Biometrisk baseret verificeringsmetode ifølge et hvilket som helst af kravene 22 til 25, yderligere omfattende et trin, hvor brugeren nægtes adgang til den ikke-flygtige hukommelse, hvis et match ikke kan identificeres på nævnte trin (c).

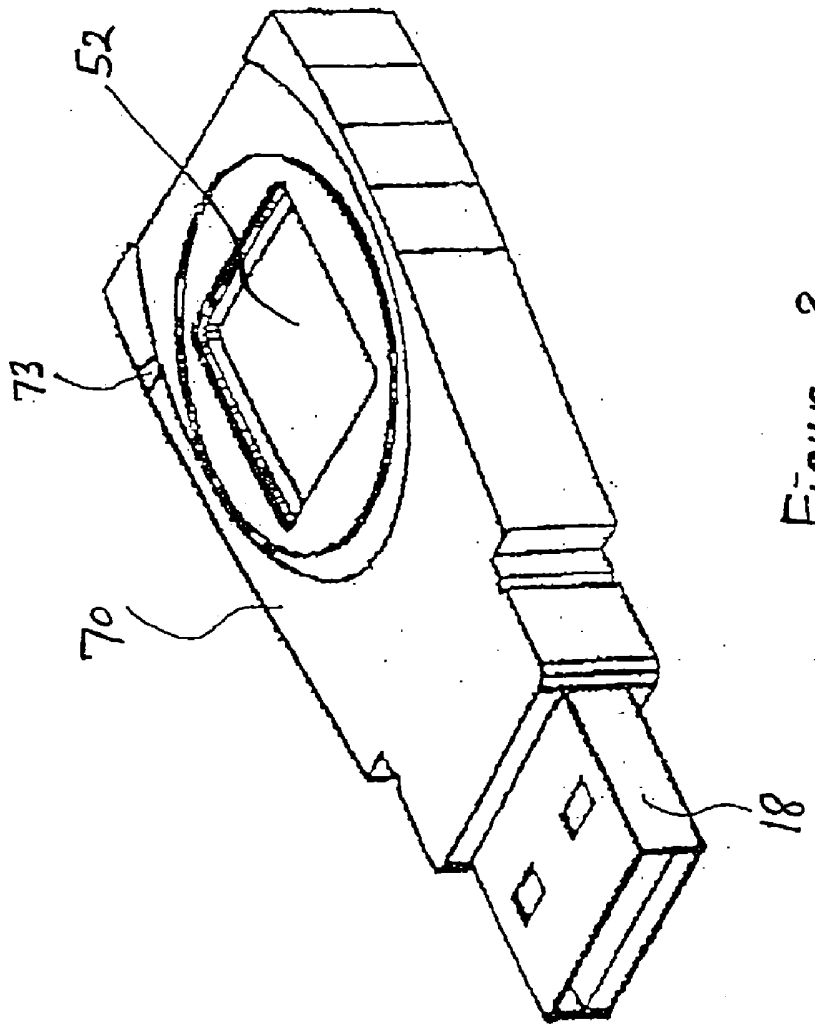
27. Biometrisk baseret verificeringsmetode ifølge et hvilket som helst af kravene 22 til 26, yderligere omfattende et trin, hvor brugeren tilbydes en alternativ verificeringsprocedure, hvis et match ikke kan identificeres på nævnte trin (c).


70
Værtsplatform 95
USB-værts-kontrolenhed 93
Elforsynings-kreds (5V/3V) 80
VCC = 3V
10
USB-kontrolenhed 15
Verificeringsmodul 12b
Skabelon-Generator 12a
Verificeringsmotor 12
RAM 16
ROM 17
Mikroprocessor 11
ECC-motor 19
Flygtig hukommelse 30
Bus-interface 13
Flash-kontrolenhed 14
Flash-hukommelse 20
Omformer 54
Sensor 52
Kontrolenhed 56
Fingeraftryksmodul 50
VCC = 3V/5V

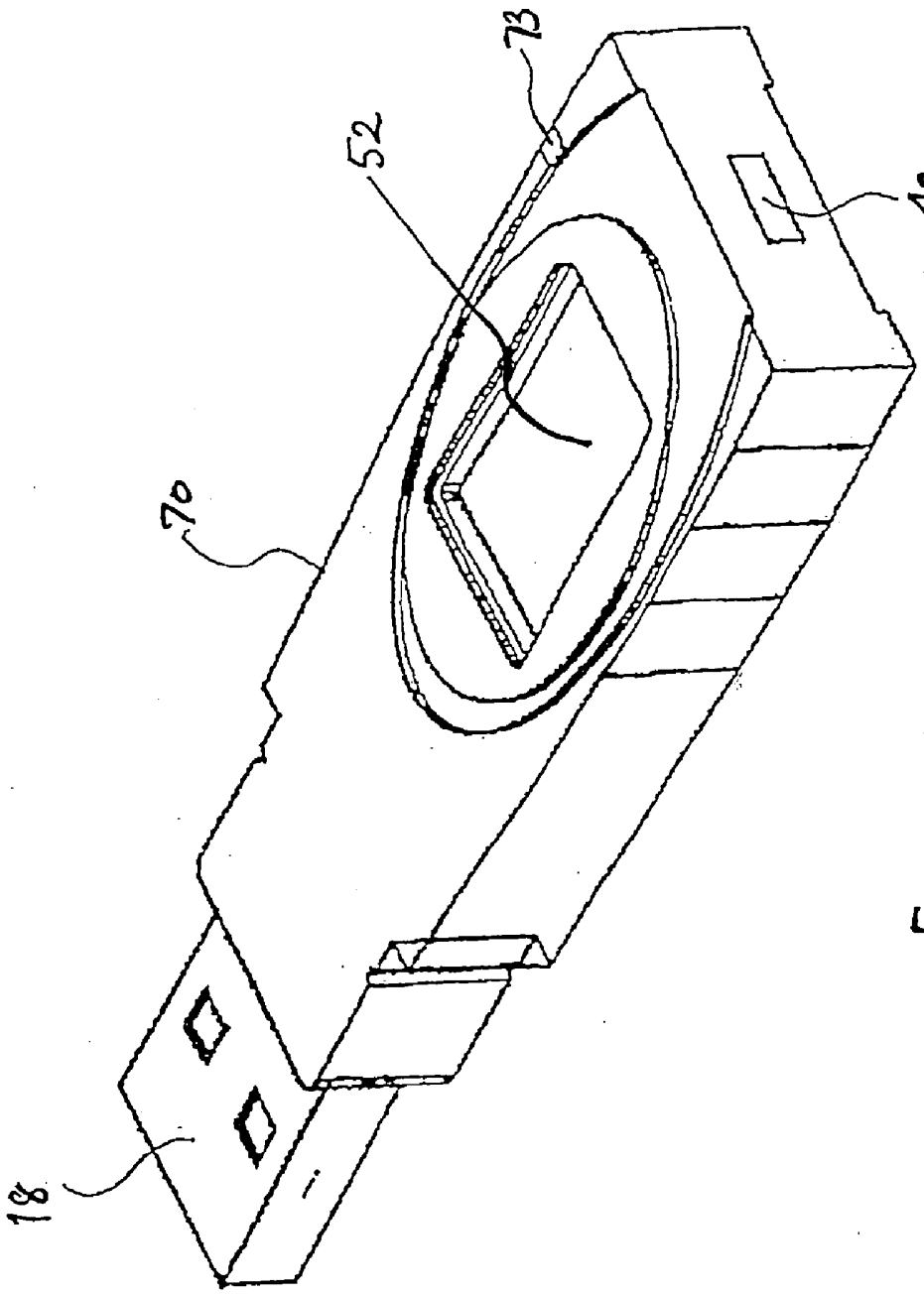
Figur 1A


Kontrolenhed 156
Sensor 152
Omformer 154
150
3
8
Hukommelses-kontrolenhed 133
Flygtig hukommelse 130
8 BIT DATA
16 BIT ADD
170
Reserveret område 122
Flag 121
Flash 120
8
Flash-kontrolenhed 114
RAM 116
ECC-motor 119
Processor 111
110
ROM 117
Læs sensor 117a
Billedbearbejdning 117b
Skabelongenerering 117c
Kryptering 117d
Verificering 117e
Skrivebeskyttelses-kontakt 140
1
1
8
5
Yderligere USB-port 162
USB-enhed
Kontrol-enhed 115
8
USB-stik
118
8
API 197
Overvågnings-software 199
USB-vært
Kontrol-enhed 193
Driver 177

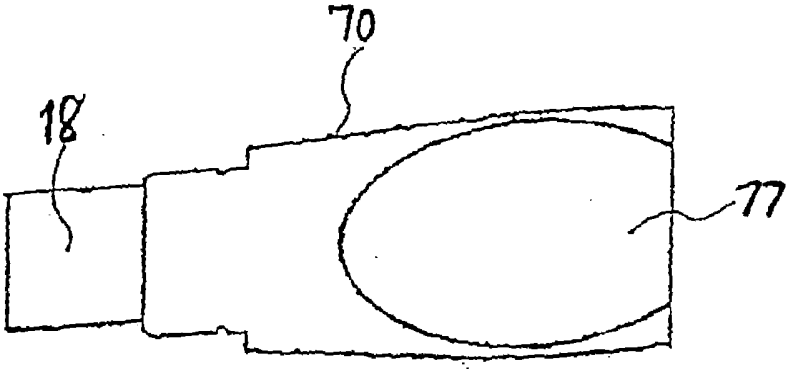
FIGUR 1B



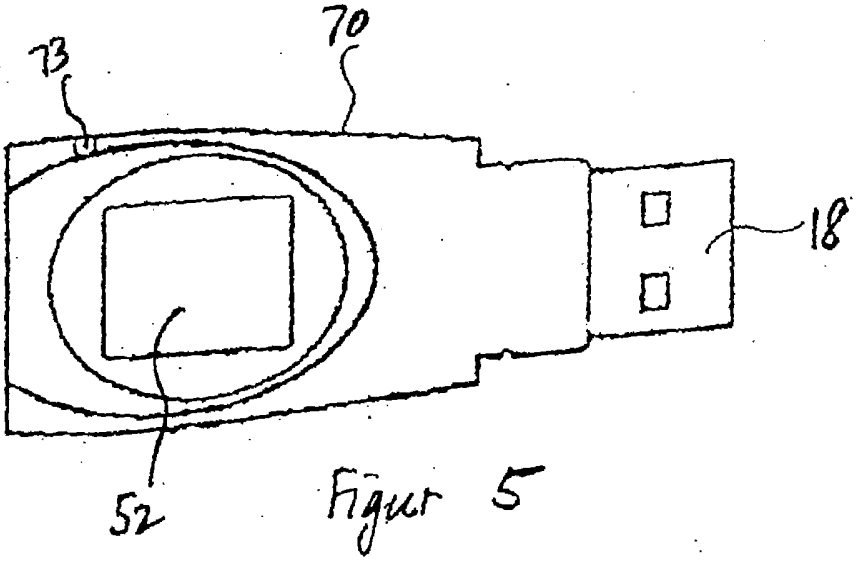
Figur 2



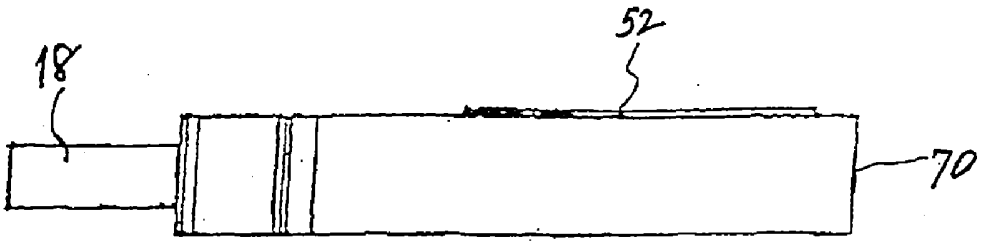
Figur 3



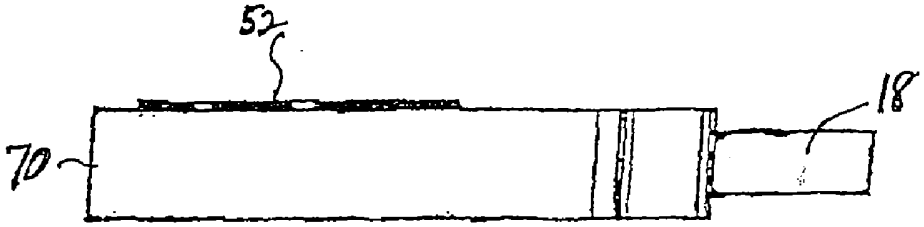
Figur 4



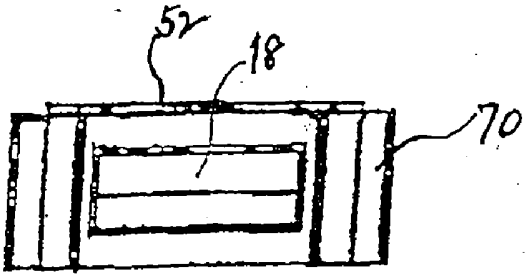
Figur 5



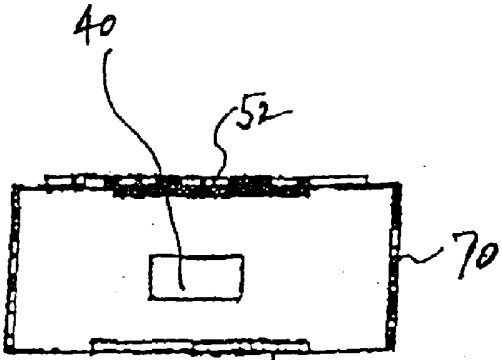
Figur 6



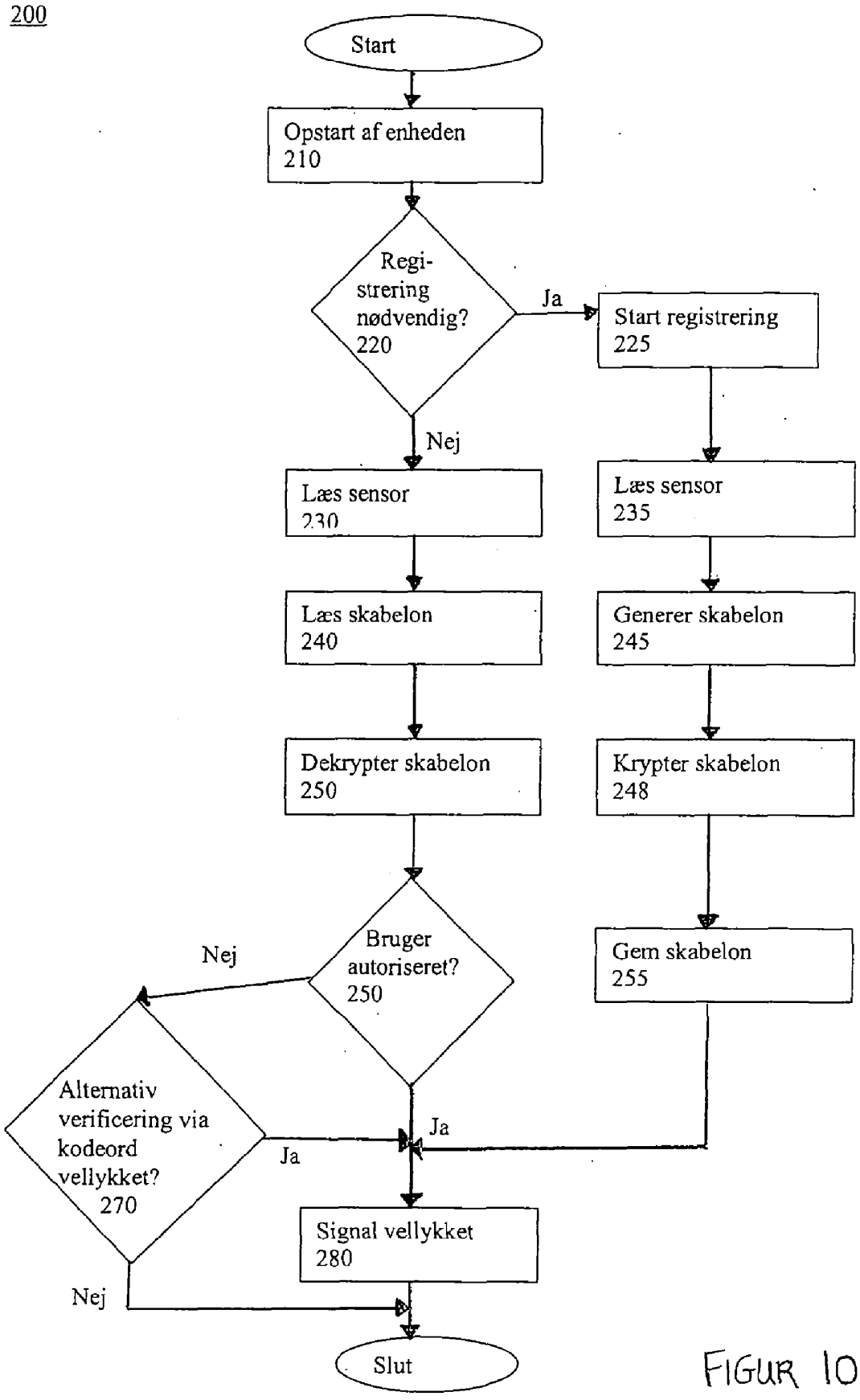
Figur 7



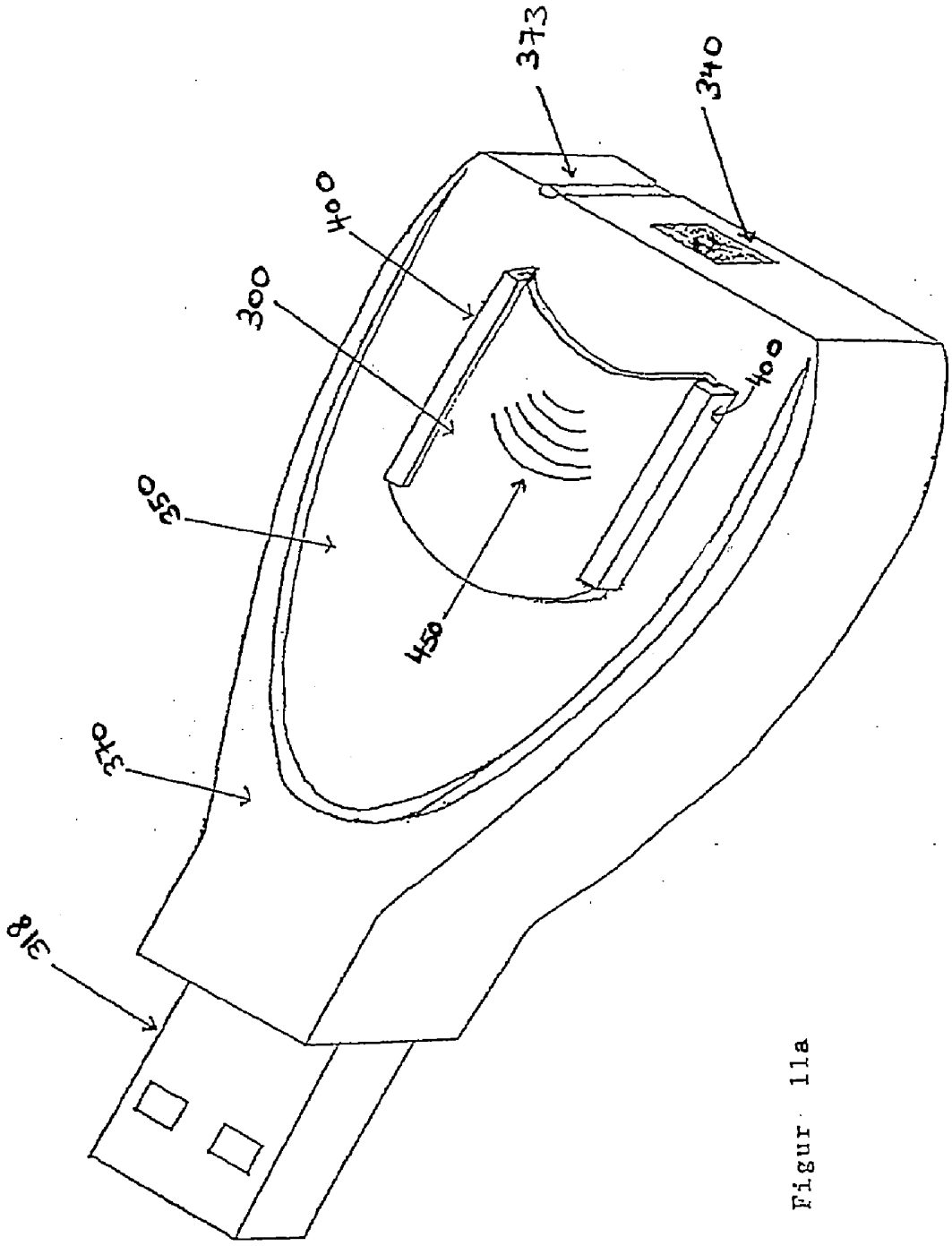
Figur 8



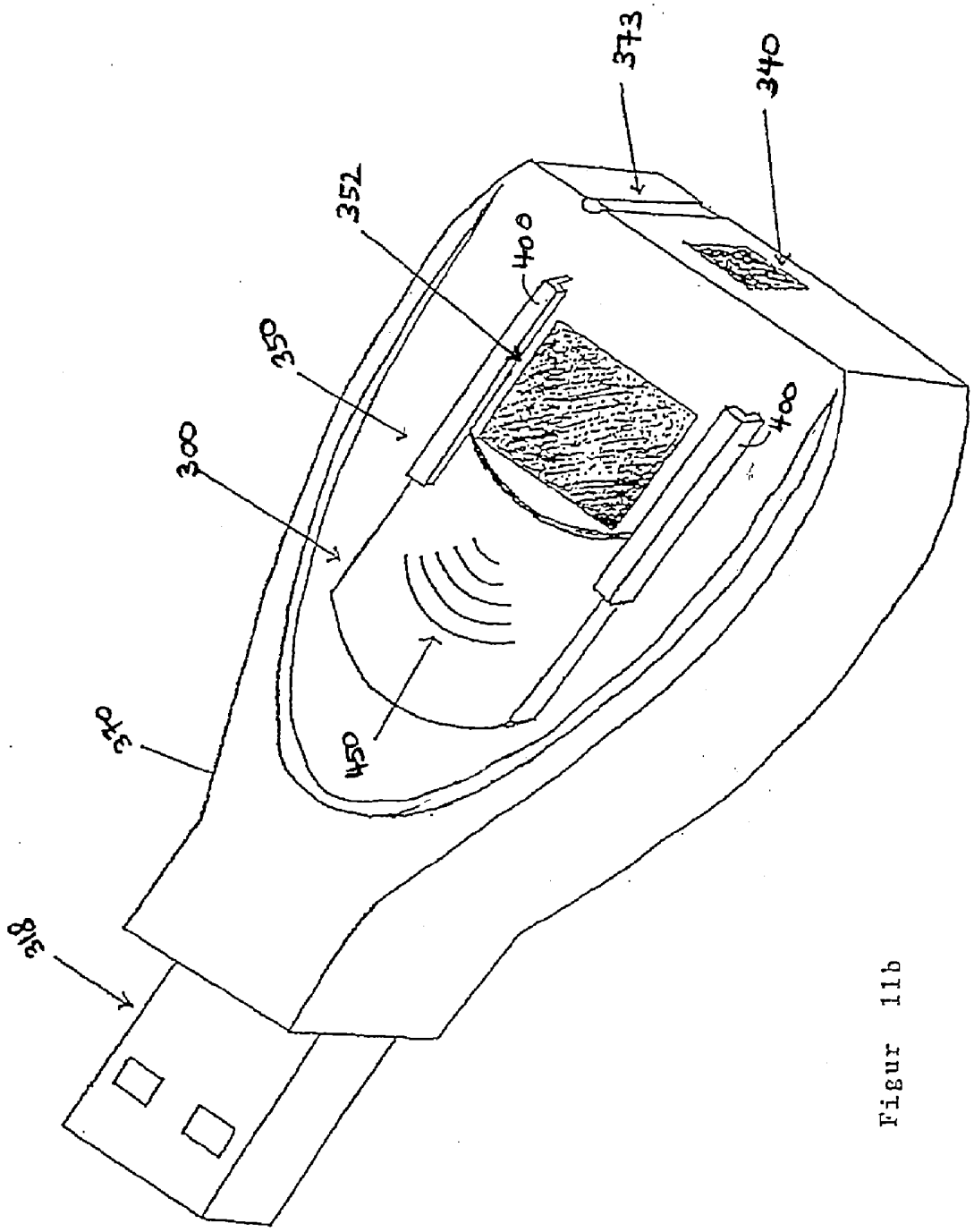
Figur 9


200
Start
Opstart af enheden
210
Regi-
strering
nødvendig?
220
Ja
Start registrering
225
Nej
Læs sensor
230
Læs sensor
235
Læs skabelon
240
Generer skabelon
245
Dekrypter skabelon
250
Krypter skabelon
248
Bruger
autoriseret?
250
Nej
Gem skabelon
255
Alternativ
verificering via
kodeord
vellykket?
270
Ja
Ja
Signal vellykket
280
Nej
Slut

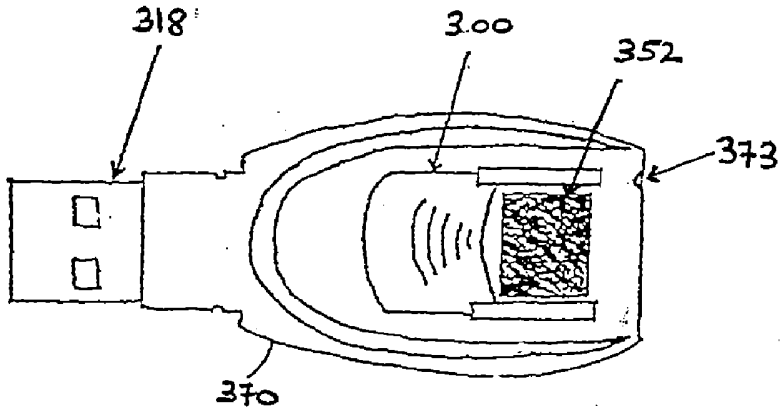
FIGUR 10



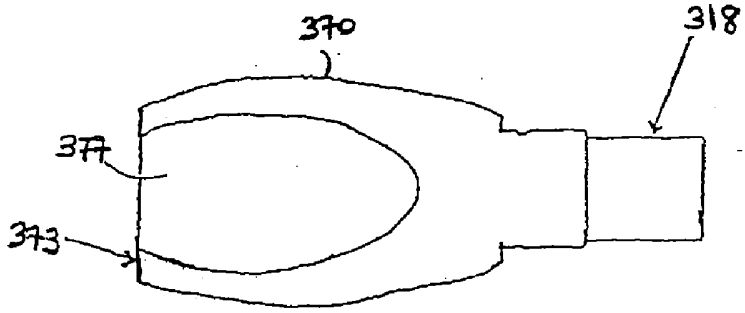
Figur 11a



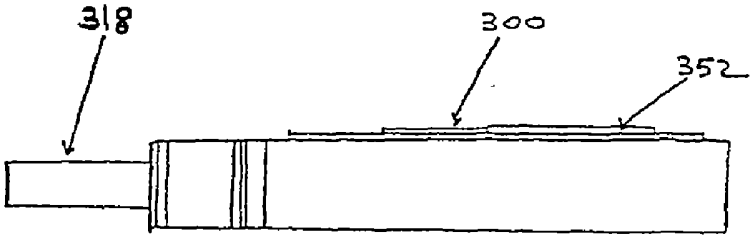
Figur 11b



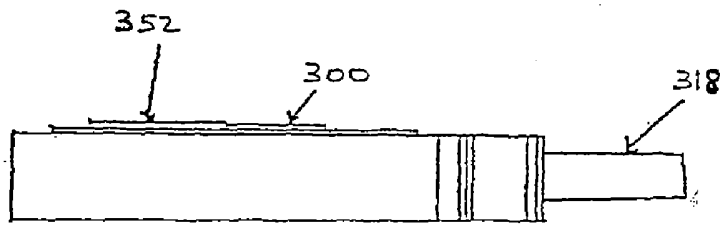
Figur 12



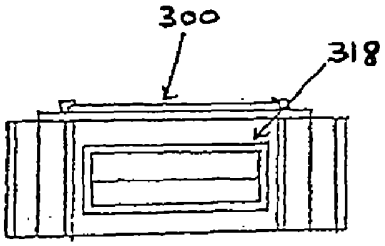
Figur 13



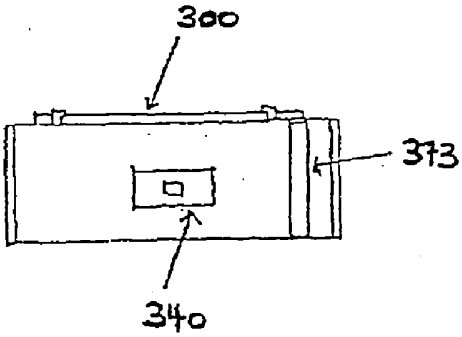
Figur 14



Figur 15



Figur 16



Figur 17