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

(11) **EP 1 454 303 B9**

(12) **CORRECTED EUROPEAN PATENT SPECIFICATION**

(15) Correction information:
Corrected version no 1 (W1 B1)
Corrections, see
Description Paragraph(s) 6
Claims EN 1

(48) Corrigendum issued on:
12.09.2012 Bulletin 2012/37

(45) Date of publication and mention of the grant of the patent:
28.03.2012 Bulletin 2012/13

(21) Application number: **01274860.4**

(22) Date of filing: **06.12.2001**

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

(86) International application number:
PCT/CA2001/001736

(87) International publication number:
WO 2003/049042 (12.06.2003 Gazette 2003/24)

(54) **PORTABLE DEVICE AND METHOD FOR ACCESSING DATA KEY ACTUATED DEVICES**

TRAGBARES GERÄT UND VERFAHREN FÜR DEN ZUGRIFF AUF PER DATENSCHLÜSSEL BETÄTIGTE VORRICHTUNGEN

DISPOSITIF PORTATIF ET PROCEDE D'ACCES A DES DISPOSITIFS COMMANDES PAR DES CLES DE DONNEES

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR

(43) Date of publication of application:
08.09.2004 Bulletin 2004/37

(73) Proprietor: **Bioscrypt Inc.**
Mississauga,
Ontario L4W 5M1 (CA)

(72) Inventor: **HOLLINGSHEAD, Dennis W.**
Toronto, Ontario M2K 2S5 (CA)

(74) Representative: **Hall, Matthew Benjamin**
Dehns
St. Bride's House
10 Salisbury Square
London EC4Y 8JD (GB)

(56) References cited:
EP-A- 0 869 460
EP-A- 0 924 657
WO-A-98/12670
GB-A- 2 181 582
US-A- 5 131 038

EP 1 454 303 B9

Printed by Jouve, 75001 PARIS (FR)

Description

FIELD OF THE INVENTION

[0001] This invention relates to a method for accessing data key actuated devices, a portable device for accessing such key actuated devices, and a secure access system.

BACKGROUND OF THE INVENTION

[0002] Access to an increasing number of devices is controlled by data access keys. For example, access to an automated teller machine (ATM) is controlled by keypad entry of an appropriate personal identification number (PIN). Similarly, access to high security doors may be controlled by keypad entry of a pass code. Access to security systems, computer networks, and voice mail systems are also typically pass code controlled. As the number of devices which demand an access key for access increases, it becomes more difficult for a user to recall all the necessary access keys. Furthermore, the security of such key actuated devices may be compromised if the access key is not maintained in strict secrecy by the authorized user.

[0003] In US 5,131,038 a verification transceiver periodically transmits identity requests. A portable identification transceiver may receive such an identity request and, in response, retrieve encrypted parametric data (e.g. biometric information such as height and weight) of an authorized possessor from memory and transmit this data. The verification transceiver receives the transmitted, encrypted parametric data, decrypts it and compares the decrypted parametric data with measured parametric data of a possessor of the portable transceiver.

[0004] In EP Application No. 0924657, a portable device has a sensor for reading biometric data, such as a fingerprint image, from a person, and a correlator for comparing the sensed data with a previously stored reference image and determining whether there is a match. If there is a match, the device generates a numerical value, such as a cyclic redundancy code (CRC), from the stored reference image, encrypts the numerical value, and transmits it to the door of a protected property as confirmation of the person's identity. Upon receipt of this identity confirmation from the device, the door compares the received numerical value with one stored previously during registration and, on a match, grants access. In an alternate embodiment, the device first sends a user name to the door. Upon receipt of the user name from the device, the door generates a public key, and transmits the public key to the device. If the device has determined that there is a match between the sensed data and the previously stored reference image, the device encrypts the CRC that is generated using the door's public key and transmits it to the door. The door decrypts the received CRC using its private key and determines if it has a matching CRC associated with user name.

[0005] This invention seeks to overcome drawbacks of known security systems.

SUMMARY OF THE INVENTION

[0006] According to the present invention, there is provided a method for accessing data key actuated devices comprising: receiving a key actuated device identifier from a key actuated device; receiving a biometric; determining whether said received biometric is an authorized biometric; comparing said received key actuated device identifier with stored key actuated device identifiers and, on finding a matching stored key actuated device identifier and where said received biometric is an authorized biometric, retrieving a stored access key associated with said matching stored key actuated device identifier; and transmitting said retrieved access key.

[0007] According to another aspect of the invention, there is provided a portable electronic access device comprising: a biometric input; a verifier responsive to said biometric input for verifying that a biometric which is input to said biometric input matches an authorized biometric and providing a verification indication; a memory storing a plurality of access keys, each for use in accessing a key actuated device and a plurality of key actuated device identifiers, each associated with one of said plurality of access keys; a receiver for receiving a key actuated device identifier; a comparator for, responsive to a verification indication from said verifier, comparing a key actuated device identifier received from a key actuated device with said stored key actuated device identifiers and, on finding a matching stored key actuated device identifier, retrieving a stored access key associated with said matching stored key actuated device identifier; and a transmitter for transmitting a retrieved access key.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] In the figures which illustrate an example embodiment of the invention,

figure 1 is a block diagram of a secure access system made in accordance with this invention, and
figure 2 is a flow diagram for operation of the process of figure 1.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0009] Turning to figure 1, a secure access system 10 comprises a data key actuated device 12 and a portable key access device 14. The key actuated device 12 could be a high security (vehicle or installation) door, an ATM, a security system, a computer network, a voice mail system or any other device requiring a data key for access. The key access device 14 comprises a processor 20 connected for two-way communication with a transceiver 22 and for two-way communication with a memory 24. The

processor also receives signals from fingerprint input 26. Memory 24 is non-volatile and stores a plurality of access keys each for use in accessing a key actuated device. The memory also stores a plurality of key actuated device identifiers, each associated with one of the plurality of stored access keys. The transceiver 22 is wireless and may communicate with the key actuated device via radio transmissions or infrared transmissions. The key access device 14 is portable and preferably battery powered. A switch (not shown) may disconnect the battery when the device is not in use to conserve battery power.

[0010] In order to use the portable access device, a user must first be enrolled. To effect enrolment, the user must pass a digitized copy of their fingerprint to an enrolment computer. This may be accomplished by the user applying their finger to the fingerprint input 26 of the access device 14 when the device is connected via a port (not shown) to the enrollment computer so that the processor 20 of the access device is prompted to pass along the digitized fingerprint image to the enrollment computer. Alternatively, the user may apply their fingerprint directly to a fingerprint input associated with the enrolment computer. This computer then calculates a template from the user's fingerprint which is an encrypted combination of the fingerprint with a verification code. Suitable techniques for obtaining such templates from a fingerprint and a code, and for recovering a code from such a template, are described in U.S. patent No. 5,680,460 entitled BIOMETRIC CONTROLLED KEY GENERATION to Tomko et al., the contents of which are incorporated by reference herein. This template is then downloaded to the portable access device and stored in memory 24. Further, the enrolment computer stores a verification indication at an address in memory 24 indicated by the verification code. Enrollment is then completed.

[0011] Operation of the system 10 of figure 1 is described in conjunction with figure 1 along with figure 2, which illustrates program control for processor 20. Key actuated device 12 periodically transmits a device identifier. It is generally preferred that the time between such transmissions is no more than about five seconds; the range of these transmissions is preferably about two meters. When the portable access device 14 is brought within range of the transmissions of the key actuated device and is turned on, transceiver 22 will receive these transmissions and pass along the key actuated device identifier to processor 20 (block 50). If the user of the portable access device then applies their fingerprint to fingerprint input 26, the fingerprint image is also received by processor 20 (block 52).

[0012] The processor may then determine whether the fingerprint which was input is that of the authorized user. This is accomplished by the processor retrieving the template stored in memory 24 on enrollment and combining this with the newly input fingerprint from input 26. The resulting verification code is used as a memory address to memory 24. If the processor finds a verification indication at this memory address in memory 24, then the biometric is considered to be authorized (block 54). In such case, the processor compares the received key actuated device identifier with key actuated device identifiers in memory. On a match being found (block 56) the processor passes a valid user indication to transceiver 22 for transmission to the key actuated device 12 (block 58). This valid user indication could comprise the verification code, or an encrypted version of same. Additionally, the processor retrieves the access key from memory 24 which is associated with the matching key actuated device identifier (block 60).

[0013] When the key actuated device 12 receives a valid user indication from access device 14, it transmits a one time temporary encryption key. This is received by transceiver 22 and passed to processor 20. Processor 20 uses the temporary key to encrypt the retrieved access key (block 62). The encrypted access key is then passed to the transceiver 22 and transmitted to the key actuated device (block 64). The key actuated device uses a decryption key to recover the decrypted access key and, if the resulting decrypted key is a valid key, allows access to the user. Where the key actuated device is a high security door, this results in the door being unlocked. Where the key actuated device is an ATM, this would allow the user access to the device via a keypad which could be provided on the portable access device 14.

[0014] It will be apparent that since the access device 14 stores a number of key actuated device identifiers and associated access keys, device 14 may be carried around by an authorized user and used to gain access to a number different key actuated devices without need of the user to memorize a plurality of pass codes.

[0015] The portable access device may be used with an existing key actuated device by modifying the device to incorporate a transceiver in same and programming the processor of the key actuated device so that the device functions in the manner described.

[0016] A number of modifications to the system as described are possible. For example, the valid user ID may be transmitted as soon as an authorized fingerprint is received by the access device 14 in advance of determining whether the received key actuated device identifier matches one of the stored identifiers.

[0017] Optionally, for lower security applications, the portable access device does not transmit a valid user indication, nor does the key actuated device transmit any temporary keys. Instead, for such applications, on access device 14 determining that an authorized user has applied their fingerprint to the input and on finding an access key for the key actuated device, this access key is transmitted in unencrypted form to the key actuated device.

[0018] Another option is for the key actuated device 12 to send a "medium security" indicator when it wants the access device 14 to send a verification code and receive a temporary key for encrypting the access keys prior to transmission and to send a "low security" indicator, or no security indicator, when it wants the access device 14 to follow the described low security option.

[0019] A high security option is for the access keys to be encrypted in the access device 14. To accomplish this option, on enrolment, as well as forming a template from the user's fingerprint and a verification code, a template is formed from the user's fingerprint and a special key. The special key is then used to encrypt each access key. In operation, when the access device 14 receives a key actuated device identifier and a user's fingerprint, it retrieves any associated encrypted access key and both templates. If the fingerprint is that of the authorized user, the fingerprint successfully returns the verification code from the one template. This results in the access device 14 sending a verification indication to the key actuated device 12. The key actuated device responds by sending a temporary encryption key. The access device then uses the fingerprint to return the special key from the other fingerprint template and the special key is then used to decrypt the access key. The access device 14 next uses the temporary key to encrypt the access key and sends the encrypted access key to the key actuated device 12.

[0020] It will be obvious to those skilled in the art that the transmission of the retrieved access key may be protected by other cryptographic means. For example, a Public Key Infrastructure (PKI) may be used, such that the retrieved access key is first digitally signed using the private key of the user (synonymous with the special key above), and then encrypted using the public key of the key actuated device (synonymous with the temporary key above). This encrypted data package is then sent to the key actuated device. The user can thus be assured that only the appropriate authority can properly use the transmitted data (as only they have the private key of the key actuated device to decrypt the data), and the key actuated device can correspondingly ensure that the authorized user was present (by verifying the digital signature of the retrieved access key using the public key of the user). This provides strong mutual authentication between the actual user of the system and the key actuated device (rather than only between the portable access device and the key actuated device), as the digital signature can only be initiated subsequent to the user providing positive biometric authentication. This embodiment provides for not only a secure transmission line between the electronic access device and the key actuated device, but also provides a high degree of transaction accountability as the user must be present to initiate digital signing.

[0021] Other methods for the secure transmission of the retrieved access key will be obvious to those skilled in the art.

[0022] While in the described embodiment the user is authorized solely at the portable access device, it would be possible for the key actuated device to participate in this authorization. More particularly, on enrolment, the enrolment computer could simply pass the template to the portable access device and not the verification indication. In such instance, when a biometric is input to the access device, a verification code is returned and this code is passed directly (in encrypted or unencrypted form) to the key actuated device. The key actuated device could then pass the code to a central database which would use it to look up whether the code was indicative of a valid user. If so, the key actuated device would prompt the access device to continue. Further the key actuated device would only respond to any key transmitted by the access device where the key actuated device determined the user was authorized.

[0023] In circumstances where the access device is to transmit a valid user indication and the key actuated device is to respond with a temporary key, the valid user indication is conveniently the (encrypted or unencrypted) recovered verification code and the prompt from the key actuated device is conveniently the temporary key.

[0024] While device 14 is shown for use with a fingerprint input, equally any other user biometric could be employed. For example, access device 14 could scan an iris of a user.

[0025] Since any biometric verification device will have a non-zero false acceptance rate, preferably the key access devices 14 is programmed to shut down or broadcast an alarm code after a pre-deteimined number of consecutive failed verification attempts by a user.

[0026] Other modifications will be apparent to those skilled in the art and, therefore, the invention is defined in the claims.

Claims

1. A method for accessing data key actuated devices comprising:

   receiving a key actuated device identifier from a key actuated device (12);
   determining whether said received biometric is an authorized biometric;
   comparing said received key actuated device identifier with stored key actuated device identifiers and, on finding a matching stored key actuated device identifier and where said received biometric is an authorized biometric, retrieving a stored access key associated with said matching stored key actuated device identifier; and
   transmitting said retrieved access key.

2. The method of claim 1 further comprising:

   receiving a temporary key; and
   encrypting said retrieved access key with said temporary key prior to transmission of said retrieved access key.

3. The method of claim 2 further comprising:

   responsive to determining said received biometric is an authorized biometric, initially transmit-

ting a valid user indication.

4. The method of claim 3 wherein said temporary key is received subsequent to transmitting said valid user indication.

5. The method of claim 3 or claim 4 wherein said initially transmitting a valid user indication is dependent upon, finding a stored key actuated device identifier matching said received key actuated device identifier.

6. The method of any of claims 2 to 5 wherein each said stored access key is encrypted and including performing a decryption operation on a retrieved access key prior to encrypting said retrieved access key with said temporary key.

7. The method of claim 6 wherein each said stored access key is encrypted with a special key and wherein said performing a decryption operation comprises retrieving a template and attempting to recover said special key from said template utilizing said received biometric.

8. The method of any of claims 1 to 6 further comprising retrieving a template and attempting to recover a special key from said template utilizing said biometric, said special key for use in performing a cryptographic operation.

9. The method claim 8 wherein said cryptographic operation involves at least one said access key.

10. The method of any of claims 3 to 5 wherein said initially transmitting a valid user indication is dependent upon finding a stored key actuated device identifier matching said received key actuated device identifier.

11. The method of any of claims 1 to 10 wherein said determining whether said received biometric is an authorized biometric comprises utilizing a template comprising said authorized biometric and a verification code such that presence of said biometric allows recovery of said verification code.

12. A portable electronic access device (14) comprising:

a biometric input (26);
a transmitter (22) for transmitting a signal;
a receiver (22);
a memory (24);
a verifier (20) responsive to said biometric input (26) for verifying that a biometric which is input to said biometric input (26) matches an authorized biometric and providing a verification indication;

characterized in that:

said memory (24) stores a plurality of access keys, each for use in accessing a key actuated device (12) and a plurality of key actuated device identifiers, each associated with one of said plurality of access keys;
said receiver (22) receives a key actuated device identifier;

and said device (14) further comprises:

a comparator (20) for, responsive to said verification indication from said verifier, comparing a key actuated device identifier received from a key actuated device (12) with said stored key actuated device identifiers and, on finding a matching stored key actuated device identifier, retrieving a stored access key associated with said matching stored key actuated device identifier; and
wherein said signal transmitted by said transmitter (22) is said retrieved access key.

13. The device (14) of claim 12 wherein said stored access keys are encrypted and including a decrypter for decrypting a retrieved access key prior to said access key being transmitted by said transmitter (22).

14. The device (14) of claim 12 wherein said memory (24) is also for storing a special key template, said access keys are encrypted with a special key and said decrypter is responsive to said biometric input (26) to perform a special key recovery operation on said special key template utilizing said input biometric and a subsequent decrypting operation on said retrieved access key utilizing a recovered special access key.

15. The device (14) of claim 12 or claim 13 wherein said memory (24) is also for storing a special key template comprising said authorized biometric and a special key, said special key for use in performing a cryptographic operation.

16. The device (14) of any of claims 12 to 15 wherein said verifier is for accessing a stored template comprising said authorized biometric and a versification code, for attempting to recover said verification code from an input biometric and for using said verification code to obtain said verification indication.

17. The device (14) of any claims 12 to 16 wherein said receiver (22) is also for receiving a temporary key and including an encrypter for encrypting said retrieved access key with said temporary key prior to transmission of said retrieved access key by said

transmitter (22).

18. The device (14) of any of claims 12 to 17 wherein said transmitter (22) is also for initially transmitting a valid user indication in response to said verifier providing said verification indication.

19. The device (14) of claim 17 wherein said transmitter (22) is also for initially transmitting a valid user indication in response to said verifier providing said verification indication and wherein said temporary key is received after said transmitter has transmitted said valid user indication.

20. The device (14) of any of claims 12 to 19 wherein said receiver (22) comprises one of a radio receiver and an infrared receiver and said transmitter (22) comprises one of a radio transmitter and an infrared transmitter.

21. A secure access system (10), comprising:

a data key actuated device (12) for transmitting a signal;
a portable access device (14) comprising:

a biometric input (26);
a transmitter (22) for transmitting a signal;
a memory (24);
a receiver (22) for receiving said signal transmitted by said key actuated device (12);
a verifier (20) responsive to said biometric input (26) for verifying that a biometric which is input to said biometric input matches an authorized biometric and providing a verification indication;

characterized in that:

said memory (24) stores a plurality of access keys, each for use in accessing a key actuated device (12) and a plurality of key actuated device identifiers, each associated with one of said plurality of access keys; said signal transmitted by said key actuated device (12) is periodically transmitted and said signal transmitted by said key actuated device (12) is a key actuated device identifier; and

said portable device (14) further comprises:

a comparator (20) for, responsive to said verification indication from said verifier (20), comparing a key actuated device identifier received from said key actuated device (12) with said stored key actuated device identifiers and, on a match, retrieving an access key associated with said matching stored key actuated device identifier; and wherein said signal transmitted by said transmitter (22) is said retrieved access key to said key actuated device.

22. The system (10) of claim 21 wherein said receiver (22) is for receiving a temporary key and wherein said access device (14) includes an encrypter for encrypting said retrieved access key with said temporary key prior to transmission of said retrieved access key by said transmitter (22).

23. The system (10) of claim 21 or 22 wherein said transmitter (22) is also for initially transmitting a valid user indication in response to said verifier (20) providing said verification indication to said access device (14) and wherein said key actuated device (12) is also for, responsive to receiving said valid user indication, transmitting said temporary key.

24. The system (10) of any of claims 21 to 23 wherein said memory (24) is also for storing a template and wherein said verifier (20) is also for attempting to recover a special key from said template utilizing said biometric, said special key for use in performing a cryptographic operation.

25. The system (10) of any of claims 21 to 24 wherein said transmitter (22) is a radio transmitter and said receiver (22) is a radio receiver.

26. The system (10) of any of claims 21 to 25 wherein said verifier (20) is for accessing a stored template comprising said authorized biometric and a verification code, for attempting to recover said verification code from an input biometric and for using said verification code to obtain said verification indication.

Patentansprüche

1. Verfahren zum Zugreifen auf Datenschlüssel-betätigte Vorrichtungen, umfassend:

Empfangen eines Schlüssel-betätigten Vorrichtungs-Identifikators aus einer Schlüssel-betätigten Vorrichtung (12);
Empfangen einer Biometrik;
Bestimmen, ob die empfangene Biometrik eine autorisierte Biometrik ist;
Vergleichen des empfangenen Schlüssel-betätigten Vorrichtungs-Identifikators mit gespeicherten Schlüssel-betätigten Vorrichtungs-Identifikatoren und, beim Finden eines passenden gespeicherten Schlüssel-betätigten Vorrichtungs-Identifikators und wenn die empfan-

gene Biometrik eine autorisierte Biometrik ist, Abrufen eines gespeicherten Zugriffschlüssels, der mit dem passenden gespeicherten Schlüssel-betätigten Vorrichtungs-Identifikator assoziiert ist; und
Senden des abgerufenen Zugriffsschlüssels.

2. Verfahren nach Anspruch 1, weiter umfassend:

Empfangen eines zeitweiligen Schlüssels; und Verschlüsseln des abgerufenen Zugriffsschlüssels mit dem zeitweiligen Schlüssel, vor dem Senden des abgerufenen Zugriffsschlüssels.

3. Verfahren nach Anspruch 2, weiter umfassend:

in Reaktion darauf, dass festgestellt wird, dass die empfangene Biometrik eine autorisierte Biometrik ist, anfangs Senden einer gültigen Anwenderindikation.

4. Verfahren nach Anspruch 3, wobei der zeitweilige Schlüssel empfangen wird nachfolgend dem Senden der gültigen Anwenderindikation.

5. Verfahren nach Anspruch 3 oder 4, wobei das anfängliche Senden einer gültigen Anwenderindikation vom Auffinden eines gespeicherten Schlüssel-betätigten Vorrichtungs-Identifikators abhängt, der zum empfangenen Schlüssel-betätigten Vorrichtungs-Identifikator passt.

6. Verfahren nach einem der Ansprüche 2 bis 5, wobei jeder gespeicherte Zugriffsschlüssel verschlüsselt wird und das Durchführen einer Entschlüsselungsoperation an einem abgerufenen Zugriffsschlüssel vor dem Verschlüsseln des abgerufenen Zugriffsschlüssels mit dem zeitweiligen Schlüssel beinhaltet.

7. Verfahren nach Anspruch 6, wobei jeder gespeicherte Zugriffsschlüssel mit einem speziellen Schlüssel verschlüsselt wird und wobei das Durchführen einer Entschlüsselungsoperation das Wiedergewinnen einer Vorlage und den Versuch, den speziellen Schlüssel aus der Vorlage unter Verwendung der empfangenen Biometrik wiederherzustellen, umfasst.

8. Verfahren nach einem der Ansprüche 1 bis 6, weiter umfassend das Abrufen einer Vorlage und Versuchen, einen speziellen Schlüssel aus der Vorlage unter Verwendung der Biometrik wiederherzustellen, wobei der spezielle Schlüssel zur Verwendung bei der Durchführung einer kryptographischen Operation bestimmt ist.

9. Verfahren nach Anspruch 8, wobei die kryptographische Operation zumindest einen besagten Zugriffsschlüssel involviert.

10. Verfahren nach einem der Ansprüche 3 bis 5, wobei das anfängliche Senden einer gültigen Anwenderindikation vom Auffinden eines gespeicherten Schlüssel-betätigten Vorrichtungs-Identifikators abhängt, der zum empfangenen Schlüssel-betätigten Vorrichtungs-Identifikator passt.

11. Verfahren nach einem der Ansprüche 1 bis 10, wobei das Bestimmen, ob die empfangene Biometrik eine autorisierte Biometrik ist, das Verwenden einer Vorlage umfasst, die die autorisierte Biometrik und einen Verifizierungscode umfasst, so dass das Vorliegen der Biometrik das Wiederherstellen des Verifizierungscodes gestattet.

12. Tragbare elektronische Zugriffsvorrichtung (14), umfassend:

eine biometrische Eingabe (26);
einen Sender (22) zum Senden eines Signals;
einen Empfänger (22);
einen Speicher (24);
einen Verifizierer (20) der reagibel ist auf die biometrische Eingabe (26), um zu verifizieren, dass eine Biometrik, die an der biometrischen Eingabe (26) eingegeben wird, zu einer autorisierten Biometrik passt und eine Verifizierungs-Identifikation bereitzustellen;

dadurch gekennzeichnet, dass:

der Speicher (24) eine Mehrzahl von Zugriffsschlüsseln speichert, jeder zur Verwendung beim Zugreifen auf eine Schlüssel-betätigte Vorrichtung (12) und eine Mehrzahl von Schlüssel-betätigten Vorrichtungs-Identifikatoren, die alle mit einem aus der Mehrzahl von Zugriffsschlüsseln assoziiert sind;
der Empfänger (22) einen Schlüssel-betätigten Vorrichtungs-Identifikator empfängt;

und die Vorrichtung (14) weiter umfasst:

einen Komparator (20) zum Vergleichen, in Reaktion auf die Verifikationsindikation aus dem Verifizierer, eines aus einer Schlüssel-betätigten Vorrichtung (12) empfangenen Schlüssel-betätigten Vorrichtungs-Identifikators mit den gespeicherten Schlüssel-betätigten Vorrichtungs-Identifikatoren, und, beim Finden eines passenden gespeicherten Schlüssel-betätigten Vorrichtungs-Identifikators, Abrufen eines gespeicherten Zugriffsschlüssels, der mit dem passenden gespeicherten Schlüssel-betätigten Vorrichtungs-Identifikator assoziiert ist; und

wobei das durch den Sender (22) gesendete Signal der wiedergewonnene Zugriffsschlüssel ist.

13. Vorrichtung (14) nach Anspruch 12, wobei die gespeicherten Zugriffsschlüssel verschlüsselt sind und einen Entschlüsseler zum Entschlüsseln eines abgerufenen Zugriffsschlüssels beinhalten, bevor der Zugriffsschlüssel durch den Sender (22) gesendet wird.

14. Vorrichtung (14) nach Anspruch 12, wobei der Speicher (24) auch zum Speichern einer speziellen Schlüsselvorlage dient, die Zugriffsschlüssel mit dem speziellen Schlüssel, verschlüsselt sind und der Entschlüsseler auf die biometrische Eingabe (26) reaktiv ist, um eine spezielle Schlüsselwiederherstelloperation an der speziellen Schlüsselvorlage, welche die eingegebene Biometrik einsetzt, und eine nachfolgende Entschlüsselungsoperation am abgerufenen Zugriffsschlüssel durchzuführen, welche einen wiederhergestellten speziellen Zugriffsschlüssel verwendet.

15. Vorrichtung (14) nach Anspruch 12 oder Anspruch 13, wobei der Speicher (24) auch zum Speichern einer speziellen Schlüsselvorlage dient, die die autorisierte Biometrik und einen speziellen Schlüssel umfasst, wobei der spezielle Schlüssel zur Verwendung bei der Durchführung einer kryptographischen Operation dient.

16. Vorrichtung (14) nach einem der Ansprüche 12 bis 15, wobei der Verifikator zum Zugreifen auf eine gespeicherte Vorlage dient, die die autorisierte Biometrik und einen Verifizierungscode umfasst, zum Versuchen, den Verifikationscode aus der eingegebenen Biometrik wiederherzustellen, und zum Verwenden des Verifikationscodes, um die Verifikationsindikation zu erhalten.

17. Vorrichtung (14) nach einem der Ansprüche 12 bis 16, wobei der Empfänger (22) auch zum Empfangen eines zeitweiligen Schlüssels dient und einen Verschlüsseler zum Verschlüsseln des abgerufenen Zugriffsschlüssels mit dem zeitweiligen Schlüssel vor dem Senden des wieder gewonnenen Zugriffsschlüssels durch den Sender (22) beinhaltet.

18. Vorrichtung (14) nach einem der Ansprüche 12 bis 17, wobei der Sender (22) auch zum anfänglichen Senden einer gültigen Anwenderindikation in Reaktion auf den Verifikator dient, der die Verifikationsidentifikation bereitstellt.

19. Vorrichtung (14) nach Anspruch 17, wobei der Sender (22) auch zum anfänglichen Senden einer gültigen Anwenderindikation in Reaktion darauf, dass der Verifikator die Verifikationsindikation bereitstellt, bestimmt ist, und wobei der zeitweilige Schlüssel empfangen wird, nachdem der Sender die gültige Anwenderindikation gesendet hat.

20. Vorrichtung (14) nach einem der Ansprüche 12 bis 19, wobei der Empfänger (22) einen Funkempfänger oder einen Infrarotempfänger umfasst und der Sender (22) einen Funksender oder einen Infrarotsender umfasst.

21. Sicheres Zugriffssystem (10), umfassend:

eine Datenschlüssel-betätigte Vorrichtung (12) zum Senden eines Signals;
eine tragbare Zugriffsvorrichtung (14), die umfasst:

eine biometrische Eingabe (26);
einen Sender (22) zum Senden eines Signals;
einen Speicher (24);
einen Empfänger (22) zum Empfangen des durch die Schlüssel-betätigte Vorrichtung (12) gesendeten Signals;
einen Verifikator (20), der reagibel ist auf die biometrische Eingabe (26) zum Verifizieren, dass eine Biometrik, die an der Biometrikeingabe eingegeben wird, zu einer autorisierten Biometrik passt, und Bereitstellen einer Verifikationsindikation;

dadurch gekennzeichnet, dass:

der Speicher (24) eine Mehrzahl von Zugriffsschlüsseln, von denen jeder zur Verwendung beim Zugreifen auf eine Schlüssel-betätigte Vorrichtung (12) dient, und eine Mehrzahl von Schlüssel-betätigten Vorrichtungs-Identifikatoren, die alle mit einem aus der Mehrzahl von Zugriffsschlüsseln assoziiert sind, speichert;
das durch die Schlüssel-betätigte Vorrichtung (12) gesendete Signal periodisch gesendet wird und das durch die Schlüssel-betätigte Vorrichtung (12) gesendet Signal ein Schlüssel-betätigter Vorrichtungs-Identifikator ist; und

die tragbare Vorrichtung (14) weiter umfasst:

einen Komparator (20) zum Vergleichen, in Reaktion auf die Verifikationsindikation aus dem Verifizierer (20), eines aus der Schlüssel-betätigten Vorrichtung (12) empfangenen Schlüssel-betätigten Vorrichtungs-Identifikators mit den gespeicherten Schlüssel-betätigten Vorrichtungs-Identifi-

katoren, und, bei einer Passung, Abrufen eines gespeicherten Zugriffsschlüssels, der mit dem passenden gespeicherten Schlüssel-betätigten Vorrichtungs-Identifikator assoziiert ist; und wobei das durch den Sender (22) gesendete Signal der wiedergewonnene Zugriffsschlüssel zur Schlüsselbetätigten Vorrichtung ist.

22. System (10) nach Anspruch 21, wobei der Empfänger (22) zum Empfangen eines zeitweiligen Schlüssels dient und wobei die Zugriffsvorrichtung (14) einen Verschlüsseler zum Verschlüsseln des abgerufenen Zugriffsschlüssels mit dem zeitweiligen Schlüssel vor dem Senden des abgerufenen Zugriffsschlüssels durch den Sender (22) beinhaltet.

23. System (10) nach Anspruch 21 oder 22, wobei der Sender (22) auch zum anfänglichen Senden einer gültigen Anwenderindikation in Reaktion darauf dient, dass der Verifizierer (20) die Verifikationsindikation der Zugriffsvorrichtung (14) bereitstellt und wobei die Schlüssel-betätigte Vorrichtung (12) auch, reagibel auf das Empfangen der gültigen Anwenderindikation, zum Senden des zeitweiligen Schlüssels dient.

24. System (10) nach einem der Ansprüche 21 bis 23, wobei der Speicher (24) auch dem Speichern einer Vorlage dient und wobei der Verifizierer (20) auch dazu dient, zu versuchen, einen speziellen Schlüssel aus der Vorlage unter Verwendung der Biometrik wiederherzustellen, wobei der spezielle Schlüssel zur Verwendung bei der Durchführung einer kryptographischen Operation dient.

25. System (10) nach einem der Ansprüche 21 bis 24, wobei der Sender (22) ein Funksender ist und der Empfänger (22) ein Funkempfänger ist.

26. System (10) nach einem der Ansprüche 21 bis 25, wobei der Verifizierer (20) zum Zugreifen auf eine gespeicherte Vorlage, die autorisierte Biometrik und einen Verifizierungscode dient, zum Versuchen, den Verifizierungscode aus einer eingegebenen Biometrik wiederherzustellen, und zur Verwendung des Verifikationscodes, um die Verifikationsindikation zu erhalten.

Revendications

1. Procédé destiné à accéder à un dispositif actionné par une clé de données comprenant les étapes consistant à :

recevoir un identifiant de dispositif actionné par une clé en provenance d'un dispositif actionné par une clé (12) ;
recevoir une biométrie ;
déterminer si ladite biométrie reçue est une biométrie autorisée ;
comparer ledit identifiant de dispositif actionné par une clé reçu avec des identifiants de dispositifs actionnés par une clé stockés et, s'il est trouvé un identifiant de dispositif actionné par une clé stocké qui correspond et si ladite biométrie reçue est une biométrie autorisée, extraire une clé d'accès stockée associée audit identifiant de dispositif actionné par une clé stocké qui correspond ; et
émettre ladite clé d'accès extraite.

2. Procédé selon la revendication 1, comprenant en outre les étapes consistant à:

recevoir une clé temporaire ; et
chiffrer ladite clé d'accès extraite avec ladite clé temporaire avant une émission de ladite clé d'accès extraite.

3. Procédé selon la revendication 2, comprenant en outre l'étape consistant à :

en réponse à la détermination que ladite biométrie reçue est une biométrie autorisée, émettre au début une indication d'utilisateur valide.

4. Procédé selon la revendication 3, dans lequel ladite clé temporaire est reçue à la suite de l'émission de ladite indication d'utilisateur valide.

5. Procédé selon la revendication 3 ou la revendication 4, dans lequel ladite émission au début d'une indication d'utilisateur valide dépend de la découverte d'un identifiant de dispositif actionné par une clé stocké qui correspond audit identifiant de dispositif actionné par une clé reçu.

6. Procédé selon l'une quelconque des revendications 2 à 5, dans lequel chaque dite clé d'accès stockée est chiffrée, et comprenant l'exécution d'une opération de déchiffrement sur une clé d'accès extraite avant de chiffrer ladite clé d'accès extraite avec ladite clé temporaire.

7. Procédé selon la revendication 6, dans lequel chaque dite clé d'accès stockée est chiffrée avec une clé spéciale et dans lequel ladite exécution d'une opération de déchiffrement comprend l'extraction d'un modèle et une tentative visant à récupérer ladite clé spéciale à partir dudit modèle en utilisant ladite biométrie reçue.

8. Procédé selon l'une quelconque des revendications 1 à 6, comprenant en outre les étapes consistant à

extraire un modèle et à tenter de récupérer une clé spéciale à partir dudit modèle en utilisant ladite biométrie, ladite clé spéciale servant à exécuter une opération de chiffrement.

9. Procédé selon la revendication 8, dans lequel ladite opération de chiffrement implique au moins une dite clé d'accès.

10. Procédé selon la revendication 3 à 5, dans lequel ladite émission au début d'une indication d'utilisateur valide dépend de la découverte d'un identifiant de dispositif actionné par une clé stocké qui correspond audit identifiant de dispositif actionné par une clé reçu.

11. Procédé selon l'une quelconque des revendications 1 à 10, dans lequel ladite étape consistant à déterminer si ladite biométrie reçue est une biométrie autorisée comprend une étape consistant à utiliser un modèle qui comprend ladite biométrie autorisée et un code de vérification de telle sorte que la présence de ladite biométrie permette la récupération dudit code de vérification.

12. Dispositif d'accès électronique portable (14) comprenant :

une entrée biométrique (26) ;
un émetteur (22) destiné à émettre un signal ;
un récepteur (22) ;
une mémoire (24) ;
un dispositif de vérification (20) sensible à ladite entrée biométrique (26) destiné à vérifier qu'une biométrie qui est entrée dans ladite entrée biométrique (26) correspond à une biométrie autorisée, et à fournir une indication de vérification ; **caractérisé en ce que** :

ladite mémoire (24) stocke une pluralité de clés d'accès, chacune d'elles servant à accéder à un dispositif actionné par une clé (12) et une pluralité d'identifiants de dispositifs actionnés par une clé, chacun d'eux étant associé à l'une de ladite pluralité de clés d'accès ;
ledit récepteur (22) reçoit un identifiant de dispositif actionné par une clé ; et ledit dispositif (14) comprend en outre :

un comparateur (20) destiné à comparer, en réponse à ladite indication de vérification en provenance dudit dispositif de vérification, un identifiant de dispositif actionné par une clé reçu en provenance d'un dispositif actionné par une clé (12) avec lesdits identifiants de dispositifs actionnés par une clé stockés et, quand il est trouvé un identifiant de dispositif actionné par une clé stocké qui correspond, rechercher une clé d'accès stockée associée audit identifiant de dispositif actionné par une clé stocké qui correspond ; et
dans lequel ledit signal émis par ledit émetteur (22) est ladite clé d'accès extraite.

13. Dispositif (14) selon la revendication 12, dans lequel lesdites clés d'accès stockées sont chiffrées, et comprenant un dispositif de déchiffrement destiné à déchiffrer une clé d'accès extraite avant que ladite clé d'accès ne soit émise par ledit émetteur (22).

14. Dispositif (14) selon la revendication 12, dans lequel ladite mémoire (24) sert également à stocker un modèle de clé spéciale, lesdites clés d'accès sont chiffrées avec une clé spéciale et ledit dispositif de déchiffrement est sensible à ladite entrée biométrique (26) de façon à exécuter une opération de récupération de clé spéciale sur ledit modèle de clé spéciale en utilisant ladite entrée biométrique et une opération de déchiffrement ultérieure sur ladite clé d'accès extraite en utilisant une clé d'accès spéciale récupérée.

15. Dispositif (14) selon la revendication 12 ou la revendication 13, dans lequel ladite mémoire (24) sert également à stocker un modèle de clé spéciale qui comprend ladite biométrie autorisée et une clé spéciale, ladite clé spéciale servant à exécuter une opération de chiffrement.

16. Dispositif (14) selon l'une quelconque des revendications 12 à 15, dans lequel ledit dispositif de vérification sert à accéder à un modèle stocké qui comprend ladite biométrie autorisée et un code de vérification, pour tenter de récupérer ledit code de vérification à partir d'une entrée biométrique et à utiliser ledit code de vérification de façon à obtenir ladite indication de vérification.

17. Dispositif (14) selon l'une quelconque des revendications 12 à 16, dans lequel ledit récepteur (22) sert également à recevoir une clé temporaire, et comprenant un dispositif de chiffrement destiné à chiffrer ladite clé d'accès extraite avec ladite clé temporaire avant une émission de ladite clé d'accès extraite par ledit émetteur (22).

18. Dispositif (14) selon l'une quelconque des revendications 12 à 17, dans lequel ledit émetteur (22) sert également à émettre au début une indication d'utilisateur valide en réponse audit dispositif de vérification qui fournit ladite indication de vérification.

19. Dispositif (14) selon la revendication 17, dans lequel ledit émetteur (22) sert également à émettre au début une indication d'utilisateur valide en réponse

audit dispositif de vérification qui fournit ladite indication de vérification et dans lequel ladite clé temporaire est reçue après que ledit émetteur a émis ladite indication d'utilisateur valide.

20. Dispositif (14) selon l'une quelconque des revendications 12 à 19, dans lequel ledit récepteur (22) comprend l'un d'un récepteur radio et d'un récepteur infrarouge et ledit émetteur (22) comprend l'un d'un émetteur radio et d'un émetteur infrarouge.

21. Système d'accès sécurisé (10), comprenant :

un dispositif actionné par une clé de données (12) destiné à émettre un signal ;
un dispositif d'accès portable (14) comprenant :

une entrée biométrique (26) ;
un émetteur (22) destiné à émettre un signal ;
une mémoire (24) ;
un récepteur (22) destiné à recevoir ledit signal émis par ledit dispositif actionné par une clé (12) ;
un dispositif de vérification (20) sensible à ladite entrée biométrique (26) destiné à vérifier qu'une biométrie qui est entrée dans ladite entrée biométrique correspond à une biométrie autorisée, et à fournir une indication de vérification ;
caractérisé en ce que :

ladite mémoire (24) stocke une pluralité de clés d'accès, chacune d'elles servant à accéder à un dispositif actionné par une clé (12) et une pluralité d'identifiants de dispositifs actionnés par une clé, chacun d'eux étant associé à l'une de ladite pluralité de clés d'accès ;
ledit signal émis par ledit dispositif actionné par une clé (12) est émis de manière périodique et ledit signal émis par ledit dispositif actionné par une clé (12) est un identifiant de dispositif actionné par une clé ; et
ledit dispositif portable (14) comprend en outre :

un comparateur (20) destiné à comparer, en réponse à ladite indication de vérification en provenance dudit dispositif de vérification (20), un identifiant de dispositif actionné par une clé reçu en provenance dudit dispositif actionné par une clé (12) avec lesdits identifiants de dispositifs actionnés par une clé stockés et, lors d'une correspondance, rechercher une clé d'accès associée audit identifiant de dispositif actionné par une clé stocké qui correspond ; et dans lequel ledit signal émis par ledit émetteur (22) est ladite clé d'accès extraite pour ledit dispositif actionné par une clé.

22. Système (10) selon la revendication 21, dans lequel ledit récepteur (22) sert à recevoir une clé temporaire, et dans lequel ledit dispositif d'accès (14) comprend un dispositif de chiffrement destiné à chiffrer ladite clé d'accès extraite avec ladite clé temporaire avant une émission de ladite clé d'accès extraite par ledit émetteur (22).

23. Système (10) selon la revendication 21 ou la revendication 22, dans lequel ledit émetteur (22) sert également à émettre au début une indication d'utilisateur valide en réponse audit dispositif de vérification (20) qui fournit ladite indication de vérification audit dispositif d'accès (14) et dans lequel ledit dispositif actionné par une clé (12) sert également à émettre, en réponse à la réception de ladite indication d'utilisateur valide, ladite clé temporaire.

24. Système (10) selon l'une quelconque des revendications 21 à 23, dans lequel ladite mémoire (24) sert également à stocker un modèle et dans lequel ledit dispositif de vérification (20) sert également à tenter de récupérer une clé spéciale à partir dudit modèle en utilisant ladite biométrie, ladite clé spéciale servant à exécuter une opération de chiffrement.

25. Système (10) selon l'une quelconque des revendications 21 à 24, dans lequel ledit émetteur (22) est un émetteur radio et ledit récepteur (22) est un récepteur radio.

26. Système (10) selon l'une quelconque des revendications 21 à 25, dans lequel ledit dispositif de vérification (20) sert à accéder à un modèle stocké qui comprend ladite biométrie autorisée et un code de vérification, pour tenter de récupérer ledit code de vérification à partir d'une entrée biométrique et à utiliser ledit code de vérification de façon à obtenir ladite indication de vérification.

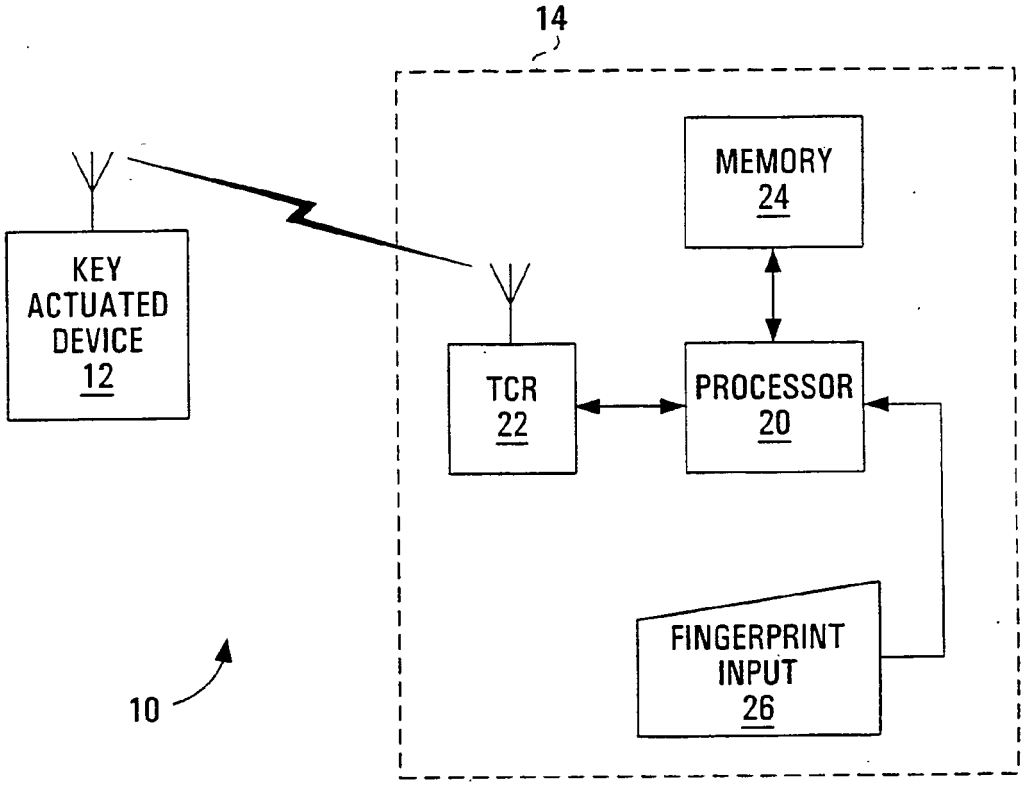
14
MEMORY
24
KEY
ACTUATED
DEVICE
12
TCR
22
PROCESSOR
20
FINGERPRINT
INPUT
26
10

FIG. 1

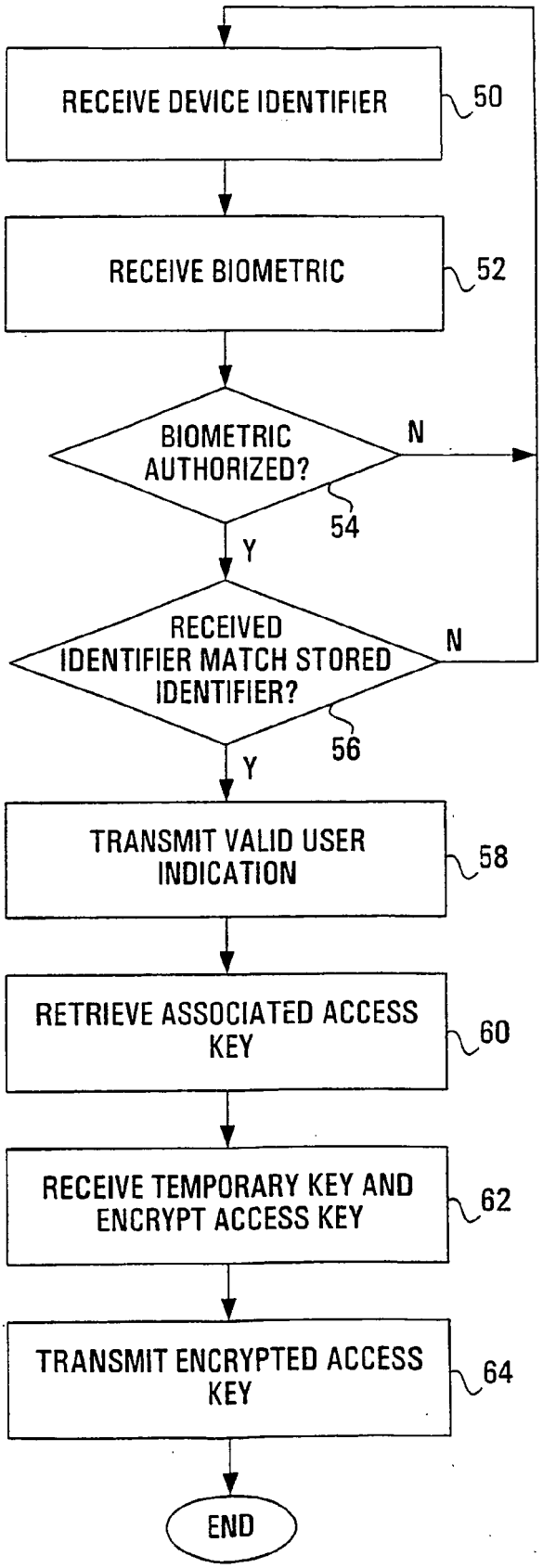
RECEIVE DEVICE IDENTIFIER
50
RECEIVE BIOMETRIC
52
BIOMETRIC AUTHORIZED?
54
N
Y
RECEIVED IDENTIFIER MATCH STORED IDENTIFIER?
56
N
Y
TRANSMIT VALID USER INDICATION
58
RETRIEVE ASSOCIATED ACCESS KEY
60
RECEIVE TEMPORARY KEY AND ENCRYPT ACCESS KEY
62
TRANSMIT ENCRYPTED ACCESS KEY
64
END

FIG. 2

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 5131038 A **[0003]**
- EP 0924657 A **[0004]**
- US 5680460 A **[0010]**