be created. The global create and delete access types are then set to the master key using the SetAccessSettings command. The DOCFilename database is then loaded in the personal key 200, and the CreateDir and CreateFile APIs 260 are used as required to create and allocate directories and files. The SelectFile, WriteFile, and CloseFile API commands are used to load the files and the secret. Depending on whether access is to be limited to a particular number of occasions, the DATA or CTR file types are used.

The BUILDOC program is used to accept new documents into the secure access library. Using information from the personal key 200, encryption keys are generated that are used by a document encryption engine in the personal key 200.

The BUILDOC program is a stand-alone application that runs on trusted systems within the secure walls of the organization. It requires validation of the master key. It uses the personal key 200 to create an encryption key for each document file name.

First, the HashToken API 260 with the XOR option is used to hash together the DOCFilename, block number (computed by the BUILDOC program as it reads and encrypts the document), DOCSecret. The block number is calculated by the BUILDOC program as it reads and encrypts the document. The resulting MD5-XOR digest is used as the encryption key that is used by the encryption engine in the BUILDOC application. Then, the CreateFile, SelectFile, WriteFile, and CloseFile APIs 260 along with the HashToken in XOR mode are used on each document that is to be added to the secure document library.

The VIEWDOC program is a web browser 262 plug-in application allows the user to open, decrypt, an view the document based on his/her personal key 200 based document access codes. If desired, the view counters for some types of documents can also be decremented in the VIEWDOC program. The VIEWDOC program does not require file saving or forwarding, screen scraping, and printing.

The VIEWDOC program validates the user and uploads and decrypts the documents. It uses the VerifyPIN command API 260 to authenticate the user. The

user can then view the documents listed in the personal key 200 directory as long as the personal key 200 remains communicatively coupled to the USB port 130.

A message facility, such as the message facility used in the WINDOWS operating system (WM_DEVICECHANGE) can be used to determine if the key has been removed. The Dir, SelectFile, ReadFile, and CloseFile command APIs 260 are used to determine which documents can be read. The HashToken with the XOR mode API 260 along with DOCSecret, DOCFilename, and the document block numbers are used to create the decryption key on a per block basis. When the DOCfilename is of file type CTR, the CTR is decremented using the Decrement command API 260. In one embodiment, to reduce complexity, the CTR field is not hashed, but merely managed by VIEWDOC.

The LIBDOC program provides an administrative function that is a subset of SETKEY. It allows a secure document librarian to grant access to documents based upon information stored in the personal key 200. The net effect is that the trusted librarian can update the personal key 200 based list of documents that can be viewed.

The LIBDOC program updates the list of DOCFilenames on a per-personal key 200 basis. After verifying the master key with VerifyMasterKey command API 260 and looking the user name up in the employee data base, the current set of DOCFilenames are updated using the SelectFile, WriteFile, and CloseFile command APIs 260.

Using the foregoing, employees worldwide can carry a personal key 200 loaded with their local database of file names. Individual departments do not have to rely on MIS procedures to restrict who has access to documents. The personal keys 200 of department members can be updated using the LIBDOC program as required. Documents can be decrypted and viewed by the employees only if the personal key 200 secret is correct. The personal secret remains secure because it is never revealed outside of the personal key 200. A simple form of metering can also be used to reduce the number of copies of documents that can be used to reduce the number of copies of documents that can be viewed.

FIG. 6 is a diagram presenting an illustration of one embodiment of the personal key 200. The personal key 200 comprises a first housing member 602 and a second housing member 604. The first housing member 602 is sized and shaped so as to accept a circuit board 606 therein.

The first housing member 602 comprises a plurality of bosses 624, which, when inserted into each respective hole 640 in the second housing member 604, secures the first housing member 602 to the second housing member 604. The first housing member 602 and the second housing member 604 also each comprise an aperture 628, which allows the personal key 200 to be affixed to a key chain.

The circuit board 606 is held in position by a plurality of circuit board supports 608. The circuit board 606 comprises a substantially flat circuit connection surface 610 on the periphery of the circuit board 606 for communicative coupling with the host processing device or computer 102 via conductive pins. Circuit connection surface 610 allows communication with a processor 212 mounted on the circuit board 606. The processor 212 comprises memory and instructions for performing the operations required to implement the functionality of the personal key 200 as disclosed herein. The processor is communicatively coupled with a memory 214 on the circuit board to store and retrieve data as required by processor 212 instructions. In the illustrated embodiment, the circuit board 606 also comprises an output device 222 such as a light emitting device 616, e.g. light emitting diode (LED), which provides the user of the personal key 200 a visual indication of the operations being performed by the personal key 200. This is accomplished, for example, by emitting light according to a signal passing from the host computer 102 to the personal key 200. The light emitting device could also comprise a liquid crystal display (LCD) or other device providing a visual indication of the functions being performed in the personal key or data passing to or from the personal key 200.

The energy from the light emitting device 616 is presented to the user in one of two ways. In the embodiment illustrated in FIG. 2, the light emitting device 616 is disposed through a light emitting device orifice 644 in the second housing member 604. In this design, the personal key 200 can be sealed with the addition of a small

amount of epoxy or other suitable material placed in the light emitting device orifice 644 after assembly.

In another embodiment, the light emitting device 616 does not extend beyond the interior of the housing 602, 604, and remains internal to the personal key 200. In this embodiment, at least a portion of the first housing 602 or the second housing 604 is at least partially translucent to the energy being emitted by the light emitting device 616 at the bandwidths of interest. For example, if the light emitting device 616 were a simple LED, the second housing 604 can be selected of a material that is translucent at visual wavelengths. One advantage of the foregoing embodiment is that the LED can be placed where it does not allow electromagnetic discharges and other undesirable energy to the circuit board 606 or any of the components disposed thereon. This is because no part of the LED, even the surface, is in contact with the user's hand at any time.

While the foregoing has been described with a single light emitting device 646, the present invention can also advantageously embody two or more light emitting devices, or devices emitting energy in other wavelengths. For example, the foregoing can be implemented with a three color LED (red, yellow and green), or three one-color LEDs to transfer personal key 200 information to the user.

In addition to or as an alternative to the foregoing, information regarding the operation of the personal key 200 is provided by an aural transducer such as a miniaturized loudspeaker or piezoelectric transducer. Such aural information would be particularly beneficial to users with limited or no vision. For example, the aural transducer can be used to indicate that the personal key 200 has been inserted properly into the host computer 120 I/O port 130.

An aural transducer may also be used to provide alert information to the user. This is particularly useful in situations where the user is not expecting any input or information from the key. For example, if the personal key 200 or related device is engaged in lengthy computations, the aural transducer can indicate when the process is complete. Also, the aural transducer can indicate when there has been an internal fault, when there has been an attempt to compromise the security of the key with

infected or otherwise harmful software instructions, or to prompt the user to take an action such as providing an input to the key 200.

Further, it is envisioned that as the use of personal keys 200 will become widespread, it will be beneficial to incorporate the functions of other devices within the personal key. For example, a device such as a paging transceiver can be incorporated into the personal key to allow the user to be summoned or contacted remotely. Or, the personal key 200 may be used to store programs and instructions such as the user's calendar. In this application, the personal key 200 can be used to remind the user of events on the calendar, especially in conjunction with the LCD display discussed above. The aural transducer can be operated at a wide variety of frequencies, including minimally audible vibrational frequencies. This design is particularly beneficial, since the personal key is small enough to be placed on the user's key ring, where it will be in pocket or purse for lengthy periods of time where it cannot be seen or easily heard.

FIGs. 7A-7C are diagrams showing one embodiment of the personal key 200 having an input device 218 including a first pressure sensitive device 702 and a second pressure sensitive device 704, each communicatively coupled the processor 212 by a communication path distinct from the USB-compliant interface 204.

FIG. 7A illustrates an embodiment of the personal key 200 in which an output device 222 such as an LED or LCD display 706 is communicatively coupled to the processor 212 by a second communication path distinct from the USB-compliant interface 204. In this embodiment, input to the personal key processor 212 may be supplied by depressing a combination of the pressure sensitive devices 702, 704, optionally as directed by the output device 222.

In an embodiment illustrated in FIGs. 7B and 7C, the pressure sensitive devices 702 and 704 are simple mechanical push switches communicatively coupled to the processor 212 via traces on the circuit board 606. In this case, the switches 702 and 704 may be actuated by depressing a button surface that extends through apertures 708 and 710 in the second housing member 604. FIG. 7B also shows a window 712 permitting viewing of the output device 706 display.

FIG. 7C shows the exterior appearance of this embodiment of the personal key 200 when the first housing member 602 and the second housing member 604 are assembled.

In another embodiment of the present invention, the pressure switches 702 and 704 do not extend to the exterior of the personal key 200. Instead, the personal key 200 is configured so that pressure may be exerted on the pressure sensitive switches 702 and 704 without requiring any portion of the switches to extend to the exterior of the personal key 200. For example, in one embodiment, at least a portion of the exterior surface of the personal key 200 is sufficiently flexible to permit pressure exerted on the outside surface of the key 200 to actuate the switches therein. Alternatively, the first housing member 602 and the second housing member 604 may be hinged to allow pressure to be applied to the switch. In another embodiment, the thresholded output of a pressure sensitive device such as a strain gauge is used to indicate user input to the personal key.

The foregoing pressure sensitive devices 702 and 704 may be used as follows. In one embodiment, the two pressure sensitive devices 702 and 704 is used to enter alphanumeric information. Here, pressure can be applied to the first pressure sensitive device 702 to select the desired character. To assist the user, the currently selected character can be displayed on the output device 222. When the user is satisfied with the selected character, applying pressure to the second pressure sensitive device may indicate that the currently displayed character should be entered (thus providing an "enter" function). This process may be repeated until all of the characters of the user input (e.g. a user password or personal identification number (PIN) has been entered. The end of the user input can be signified by repeated application of pressure to the second pressure sensitive device 702, and confirmed by the output device 222. An aural transducer can be used alone or in combination with a visual display to indicate the character, to indicate an error, or to indicate when the user input process has been completed.

The foregoing pressure sensitive devices may also be used to provide a binary input to the personal key 200. For example, the user's PIN or password can be

entered by applying pressure to the first pressure sensitive device 702 and the second pressure sensitive device 704 in the proper order in rapid succession. In this way, a user password or PIN defined as "10100010111" may be entered by depressing the first pressure sensitive device 502 to indicate a "0" and the second pressure sensitive device 704 to indicate a "1."

FIGs. 8A-8C are diagrams presenting an illustration of another embodiment of the present invention. In this embodiment, the input device 218 comprises an edge exposed wheel 802 coupled to the processor by the input device communication path 808. In this embodiment, the user provides an input by urging the wheel 802 through a series of tactile positions identifying input characters. When the desired input character is either shown on the output device 222 or on the wheel 802 itself, the user can indicate the character as a user input by urging the wheel 802 toward the centerline of the personal key 200. This process can be repeated for a series of input characters, until all of the desired characters are provided. The user can also indicate that no more input will be provided by urging the wheel 802 toward the center of the personal key multiple times in rapid succession, or by selecting an input tactile position on the wheel 802 and depressing the wheel 802.

Security Features Using the Input and Output Devices

The input device 218 and output device 222 of the present invention can be advantageously used to enhance the security of the personal key 200. For example, when connected to the host computer 102, the personal key 200 can be used to authorize transactions with a remote computer/server 134 communicatively coupled to the host computer 102 via a communication medium 132 such as a dial-up network, the Internet, LAN, or WAN. Malicious software, which can be executing in the remote computer/server 134 or the host computer 102, can send anything it wants to the personal key 200 for authorization without the knowledge or permission of the user. Without some sort of user input device 218, the personal key 200 can authorize transactions without the user's knowledge that the holder cannot repudiate. Such transactions may include, for example, payment and legally binding signatures.

Although a personal identification such as the personal identification number (PIN) is required to log on and activate the personal key 200, the personal key 200 ordinarily remains active once the PIN has been entered. Hence, the personal key 200 will perform any action for any application, without notice to, or authorization by the user.

To ameliorate this problem, one embodiment of the present invention utilizes a "squeeze to sign" authorization technique, in which some direct user action is required to authorize the use of identified secret values stored in the personal key 200. For instance, if a private key (such as the secret 406) or PIN stored in the memory 214 of the personal key 200 is identified as requiring a "squeeze to sign" authorization, firmware executing in the processor 212 of the personal key 200 requires direct user input via the input device 410 or the data transceiver 252 before honoring any request from the host computer 102 or the remote computer/server 134 that involves the use of the private key or personal information. Ordinarily, the private key and/or other personal information is designated as requiring direct authorization by an associated value or flag in the memory 214. Such data may also be designated as "use-only" indicting that the data cannot be read directly from the key under any circumstances. The data may be shared with no other entity (as would often be the case with a PIN), or may be a value shared with the trusted entity and used for authorization, such as the secret 406. For example, private keys can be used as the secret 406 to perform authorization via hash functions. In such cases, the secret value 406 is typically a shared secret such as a DES key or a password. Since secret values 406 can be stored in the memory 214 of the personal key 200, before distributing the personal key 200 to the user, the secret value 406 need not be made available in plaintext form at any time.

Typically, each time a user connects to an SSL secured web site that supports client authentication, a browser 262 calls middleware such as one of the APIs 260 or the PKCS 264, which commands the personal key 200 to encrypt a challenge value with the user's secret private key 406B (stored in the personal key memory 214). Assuming the user's PIN is already stored in the personal key 200, thus authenticating the user to the personal key 200, it still remains to authenticate the key to the secure

web site. In this case, access to the user's secret private key is required, and the output device 222 integrated with the personal key 200 may activate to indicate that a command that requires access to the private key has been invoked, and that the user needs to authorize this access. In one embodiment of the present invention this is accomplished by blinking a visual output device (such as an LED or LCD display), or by beeping an aural device. In another embodiment of the present invention, the middleware (either the API 260 or the PKCS 264) activates the display 122 attached to the computer 102, indicating that the user must authorize access to the private key before processing can proceed. An input device 218 in the personal key 200 such as the wheel 802 or one of the pressure sensitive devices 702 and 704 can then be actuated by the user to indicate that the user has authorized access to the private key. No authorization is granted if the personal key 200 is removed from the I/O port 130, or a "cancel" button presented on the display 122 is selected to refuse the on-screen dialogue. Access to the private key (in the example above, to perform the hash function) is granted if the user authorizes as such. The "squeeze to sign" concept thus makes it less likely that malicious software will be able to use the secret 406B without the user's consent or knowledge.

Malicious software may monitor the interface between the personal key 200 and the host computer 102 to capture the value of user's PIN. Although the PIN cannot be read directly, it is possible for the malicious software to examine both the VerifyPIN command described in Table 6 (and it's argument) and the response from the personal key 200. If the response indicates that the proper PIN was provided as an argument to the VerifyPIN command, the malicious software can determine the PIN itself. The foregoing can also be applied to further safeguard the user's PIN instead of the secret 406B. For example, if a sniffer module in malicious software in the host computer has been able to access the user's PIN, when it attempted to use that PIN in a context the user did not expect, the user would be alerted to the fact that the PIN had been compromised.

FIG. 9 is a flow chart illustrating an embodiment of the present invention in which processor 212 operations are subject to user authorization. First, the API 260

issues 902 a command that invokes a processor 212 operation. The command is transmitted via the USB-interface 204 to the personal key 200. The processor 212 accepts the command, as shown in block 904. The personal key 200 then determines whether the invoked processor command is one that requires authorization. This can be accomplished by storing information in the memory 214 of the personal key indicating which processor commands require authorization. For example, this can be implemented in a map stored in the memory 214, a plurality of flags, where it may be customized for each user, or the information can be stored in the processor 212 firmware or similar location so that the mapping cannot be altered. In one embodiment, different levels of authorization are implemented for different processor commands (e.g. a write command may require authorization, whereas a read command may not).

In another embodiment, authorization may be premised on data instead of the invoked command, or on a combination of the invoked command and data. For example, the present invention may be configured to require authorization any time the PIN is accessed in any way, or when the PIN is read from the memory 214 of the personal key 200, but not when other data is read, or when the PIN is written to the personal key 200. This may be accomplished, for example, by determining which data stored in the memory 214 is affected by the processor operation, and determining whether the data affected by the processor operation is associated with an identification designating the data as private information.

Using one of the output devices 222, the data transceiver 252, or the display 122 coupled to the host computer, the personal key 200 may then prompt the user to authorize the processor operation, as shown in block 906. This may be accomplished by flashing a display device such as an LED or LCD, by activating an aural transducer, or by performing both operations. If desired, the user may be prompted first with a display device, and if the authorization is not forthcoming within a specified period of time, the aural transducer may be activated.

To expose the prompting operation as little as possible to malicious software or other intrusive activity, the prompt is preferably performed using a communication

path entirely distinct from the communication path between the personal key 200 and the host computer 102 (in the illustrated example) the USB-interface 204. To further increase security, the illustrated embodiment prompts the user with the output device 222 via a communication path which not manifested externally from the personal key in any way that is visible to the malicious software, and is hence not subject to tampering.

Next, the user provides an input signaling authorization of the operation 910. This can be performed using a variety of input devices, such as the mouse 116, or keyboard 114, but is preferably performed using an input device 218 or the data transceiver 252 in the personal key 200. This information is communicated to the personal key 200 via a communication path that is entirely distinct from the communication path between the personal key 200 and the host computer 102, and preferably entirely internal to the personal key 200 (not manifested externally to the personal key 200 by a means visible to malicious software). This prevents malicious software interfering with or emulating the user authorization.

Another embodiment of the present invention provides additional PIN security. In this embodiment, the VerifyPIN command is altered from that which is described in Table 6. Ordinarily, the VerifyPIN command accepts what the host computer 102 or remote computer/server 134 believes is the user's PIN as an argument. The personal key 200 accepts this command and returns a status indicating whether the proper PIN was provided. In this alternative embodiment however, the VerifyPIN command is altered so that it does not include the PIN as an argument. The VerifyPIN command is provided to the personal key 200, and the user is prompted to enter his or her PIN. After the PIN is entered, it is communicated to the processor 212 via a communication path 220 which is distinct from the host computer 102 - personal key 200 interface, and not externally manifested anywhere where it can be detected by malicious software. It is then internally verified, and a message providing the result of that manifestation is transmitted from the personal key 200 to the host computer 200 or remote computer/server 134. This prevents any external manifestation of the PIN.

When combined with the hashing technique using the secret 406 above, the foregoing provides a highly secure technique for user authorization. The secure hashing technique authenticates the key, and protects the secret 406 from external exposure. However, the hashing technique does not authenticate the person possessing the key (since it may have been lost or stolen). The ability to enter the PIN directly into the processor 212 of the personal key allows the personal key to authenticate the user, and since the PIN is never manifested externally from the key, exposure to malicious software is prevented. Since the third party can authenticate the personal key and the personal key can authenticate the user, the third party can perform user authentication with a high degree of confidence.

FIG. 10 is a flow chart illustrating an embodiment of the present invention in which the PIN is entered directly into the personal key 200. In block 1002, a command is issued which requires access to the user's PIN, such as the VerifyPIN and ModifyPIN commands listed in Table 6. The personal key 200 accepts 1004 the command, and if necessary, prompts the user for the PIN, as shown in block 1006. This may be accomplished with the display 122, one of the output devices 222, or any combination thereof. Preferably, this is accomplished via a communication path distinct and inaccessible from the USB interface 204. Using one of the input device 218 embodiments described above, the user provides the PIN to the personal key 200. Using a value stored in the memory 214, the processor 212 in the personal key 200 validates the user-entered PIN. In one embodiment, this is accomplished by comparing the user-provided value directly with a value stored in the memory 214. The personal key then provides 1014 a response indicating the validity of the PIN, which is accepted by the API 260. The response indicates whether the user supplied PIN was valid.

In one embodiment, a biometric sensor 250 is also communicatively coupled to the processor 212. The biometric sensor 250 provides data to the processor 212 and receives commands from the processor 212, as described earlier in this disclosure.

The processor is also optionally communicatively coupled to one or more light emitting devices 216 or other visual display device to provide a visual indication of

IPR2022-00412
Apple EX1053 Page 423

the activities or status of the personal key 200. The processor 212 may also be communicatively coupled with an aural device to provide a vibrational or audio data to the user of the status or activities of the personal key 200.

Conclusion

This concludes the description of the preferred embodiments of the present invention. In summary, the present invention describes a compact, self-contained, personal token. The token comprises a USB-compliant interface releaseably coupleable to a host processing device; a memory; and a processor. The processor provides the host processing device conditional access to data storable in the memory as well as the functionality required to manage files stored in the personal key and for performing computations based on the data in the files. In one embodiment, the personal key also comprises an integral user input device and an integral user output device. The input and output devices communicate with the processor by communication paths which are independent from the USB-compliant interface, and thus allow the user to communicate with the processor without manifesting any private information external to the personal key.

The foregoing description of the preferred embodiment of the invention has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed. Many modifications and variations are possible in light of the above teaching. For example, while the foregoing personal key has been described as providing for electrical communication with the host communication, it is envisioned that such electrical communication includes the optical transfer of data such as is implemented by fiber optics and the like.

It is intended that the scope of the invention be limited not by this detailed description, but rather by the claims appended hereto. The above specification, examples and data provide a complete description of the manufacture and use of the composition of the invention. Since many embodiments of the invention can be made

without departing from the spirit and scope of the invention, the invention resides in the claims hereinafter appended.

WHAT IS CLAIMED IS:

1. A compact personal token (200), comprising:

a USB-compliant interface (206) releaseably coupleable to a host processing device (102);

a memory (214);

a processor (212), communicatively coupled to the memory (214) and communicatively coupleable to the host processing device (102) via the USB-compliant interface (130), the processor (212) for providing the host processing device (102) conditional access to data storable in the memory (214); and

a user input device (218), communicatively coupled to the processor (212) by a path (220) distinct from the USB-compliant interface (206).

2. The apparatus of claim 1, wherein the user input device (218) is configured to control an operation of the processor (212).

3. The apparatus of claim 1, wherein the operation comprises an operation selected from the group comprising:

an encryption operation; and

a decryption operation.

4. The apparatus of claim 1, wherein the operation comprises a digital signature operation using a private key stored in the memory (214).

5. The apparatus of claim 1, wherein the input device (218) comprises at least one pressure-sensitive device actuatable from an exterior surface of the token (200).

6. The apparatus of claim 1, wherein the input device (218) comprises at least one push-button switch (702).

7. The apparatus of claim 1, further comprising an output device (222), communicatively coupled to the processor (212) by path (224) distinct from the USB-compliant interface (206), for providing information regarding the operation of the processor (212).

8. The apparatus of claim 7, wherein the output device (212) comprises at least one light emitting device (616).

9. The apparatus of claim 7, wherein the output device comprises at least one liquid crystal display (706).

10. The apparatus of claim 7, wherein the output device comprises at least one aural output device.

11. A compact personal token (200), comprising:

a USB-compliant interface (206) releaseably coupleable to a host processing device (102);

a memory (214);

a processor (212), communicatively coupled to the memory (214) and communicatively coupleable to the host processing device (102) via the USB-compliant interface (206), the processor (212) for providing the host processing device (102) conditional access to data storable in the memory (214); and

a user output device (222), communicatively coupled to the processor (212).

12. The apparatus of claim 11, wherein the user output device (212) is coupled to the processor (212) by a path (224) distinct from the USB-compliant interface (206).

13. The apparatus of claim 11, wherein the user output device (212) is configured to indicate the operation of the processor (212).

14. The apparatus of claim 11, wherein the operation comprises an operation selected from the group comprising:

an encryption operation;

a decryption operation; and

a digital signature operation using a private key.

15. The apparatus of claim 11, wherein the user output device (212) is selected from a group comprising:

at least one light emitting device (616);

at least one liquid crystal display (706); and

at least one aural device.

16. The apparatus of claim 11, further comprising an input device (218), communicatively coupled to the processor (212) by path (220) distinct from the USB-compliant interface (206), for providing information for the operation of the processor (212).

17. The apparatus of claim 11, wherein the processor (212) and memory (214) are disposed on a circuit board (606) having at least one circuit connection surface (610) providing electrical communication with the processor (212), and the USB-compliant interface (206) comprises:

at least one conductive pin for providing electrical communication between the circuit connecting surface (610) and the host processing device (102), wherein the conductive pin comprises a pin securing portion and is releasably coupleable to the circuit connection surface (610); and

a housing (602) for substantially enclosing at least some of the circuit board(606), the housing (602) comprising a pin interfacing portion mateable with the pin securing portion for securing the pin member along a longitudinal axis of the conductive pin.

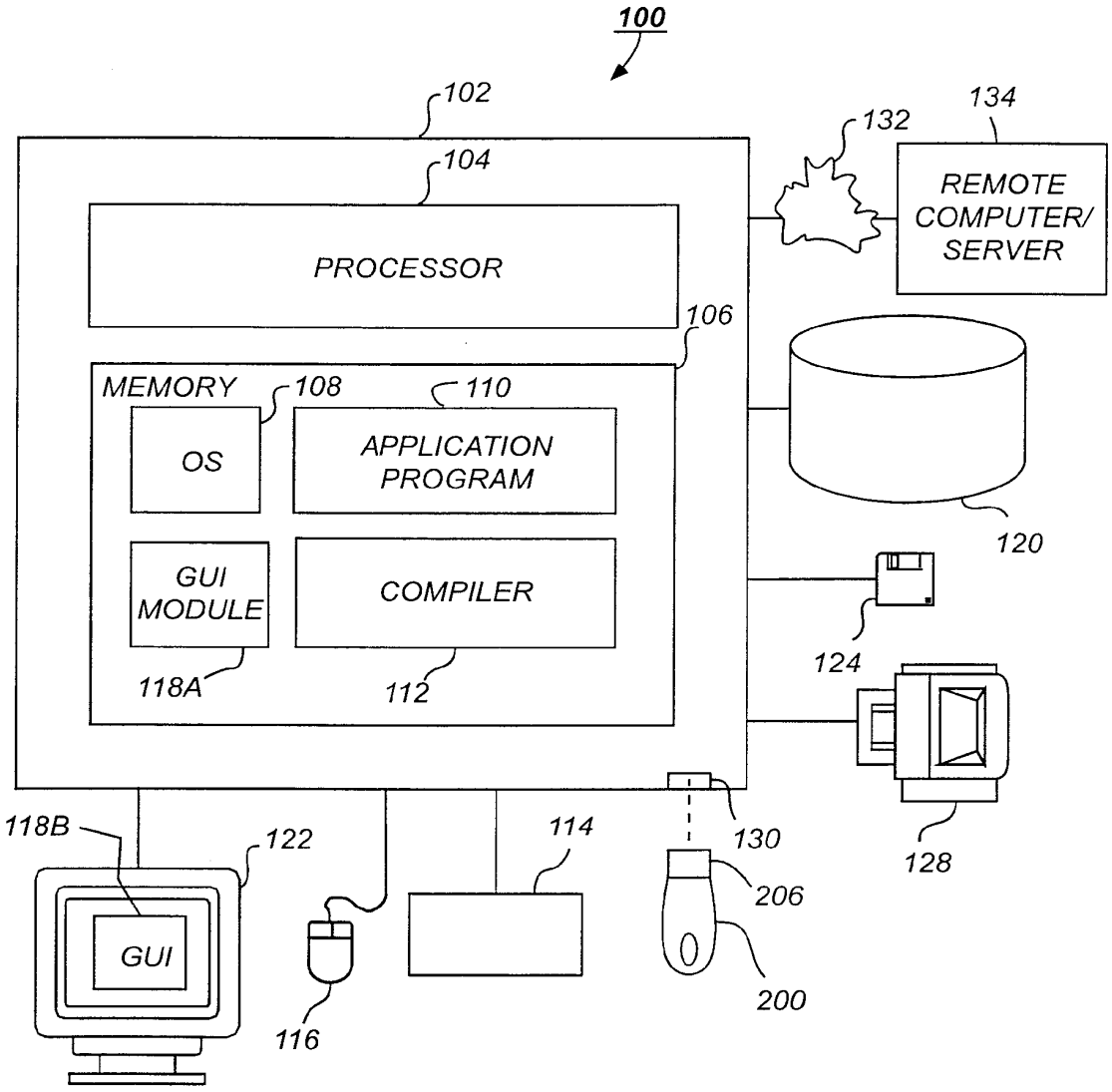

100
102
104
PROCESSOR
106
MEMORY
108
110
OS
APPLICATION PROGRAM
GUI MODULE
COMPILER
118A
112
132
134
REMOTE COMPUTER/ SERVER
120
124
128
130
206
200
114
118B
122
GUI
116

FIG. 1

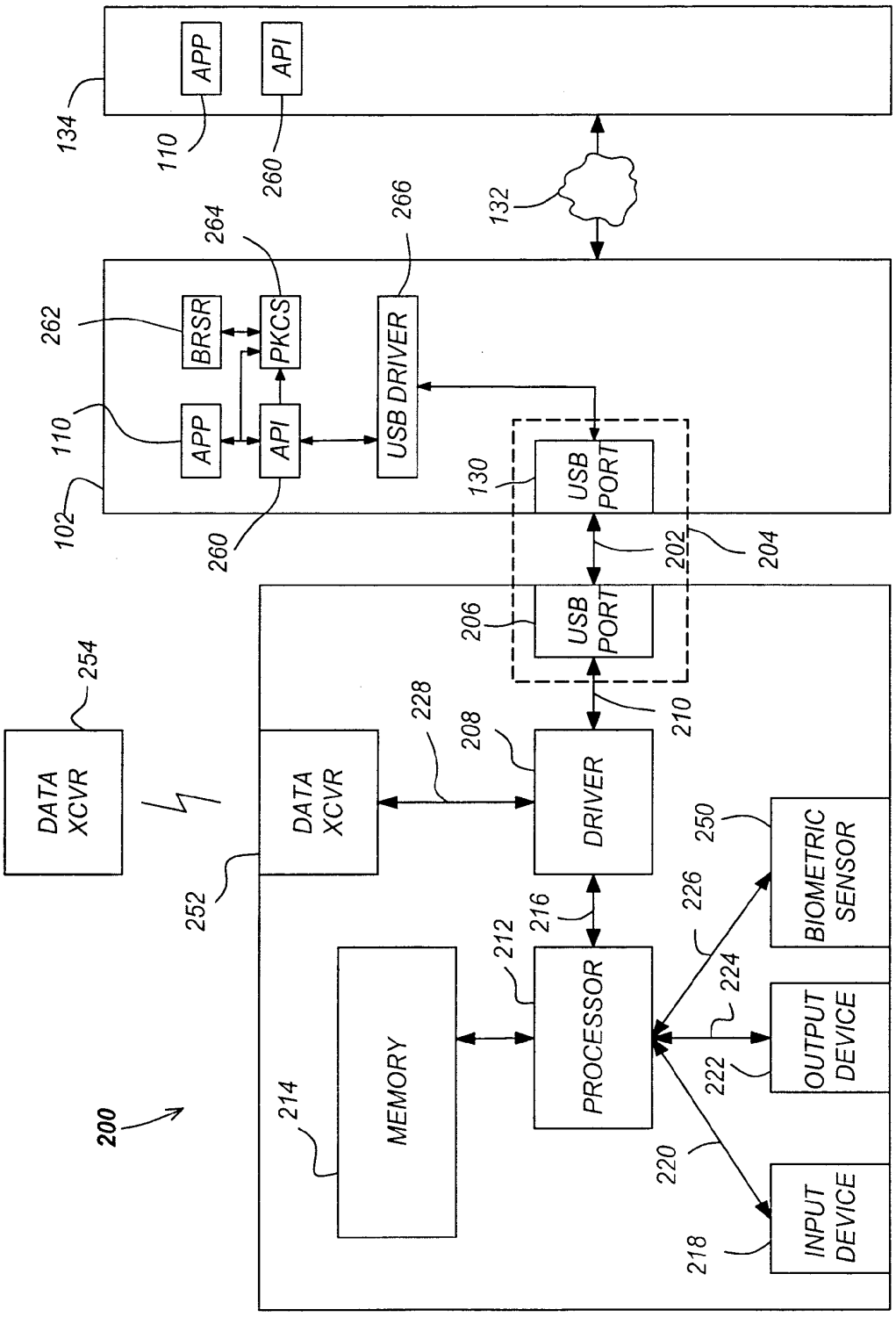

134
APP
API
110
260
132
264
266
262
BRSR
PKCS
USB DRIVER
110
APP
API
USB PORT
130
102
260
202
204
206
USB PORT
210
254
228
208
DATA XCVR
DRIVER
250
BIOMETRIC SENSOR
252
DATA XCVR
216
226
212
224
PROCESSOR
OUTPUT DEVICE
222
200
214
MEMORY
220
INPUT DEVICE
218

FIG. 2

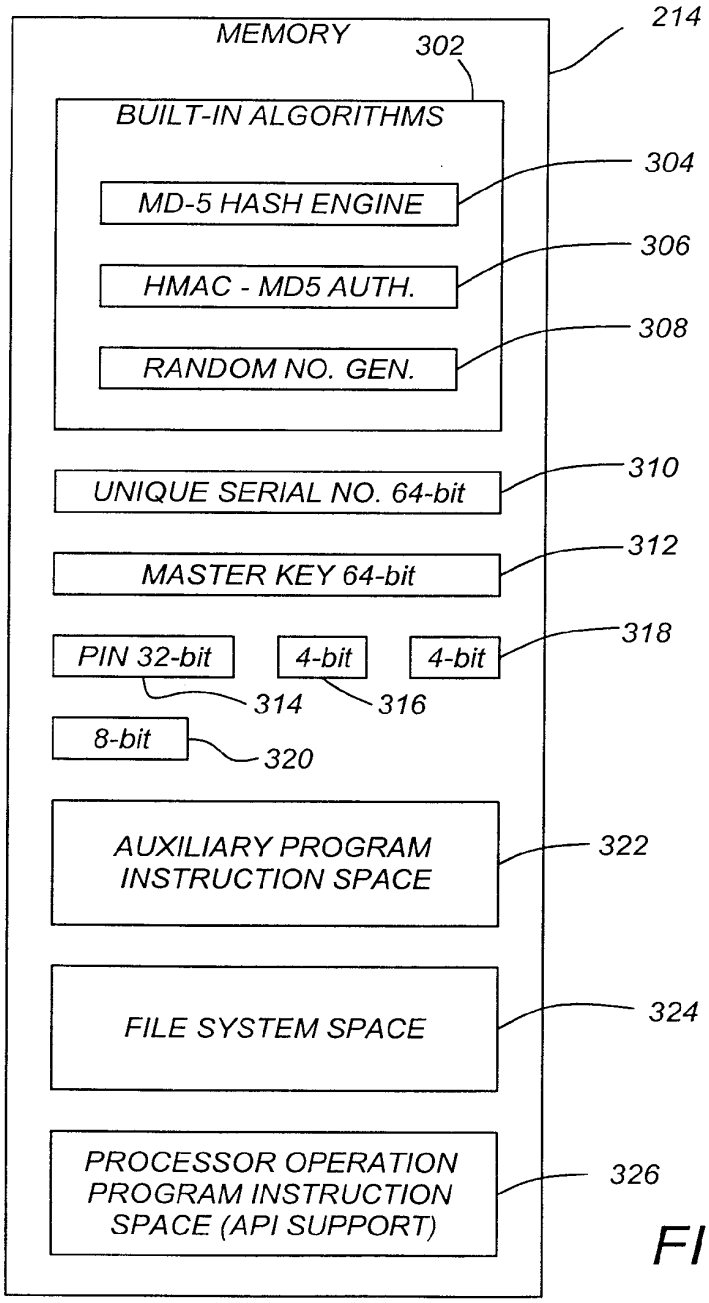

MEMORY
214
302
BUILT-IN ALGORITHMS
304
MD-5 HASH ENGINE
306
HMAC - MD5 AUTH.
308
RANDOM NO. GEN.
310
UNIQUE SERIAL NO. 64-bit
312
MASTER KEY 64-bit
318
PIN 32-bit
4-bit
4-bit
314
316
8-bit
320
AUXILIARY PROGRAM INSTRUCTION SPACE
322
FILE SYSTEM SPACE
324
PROCESSOR OPERATION PROGRAM INSTRUCTION SPACE (API SUPPORT)
326

FIG. 3

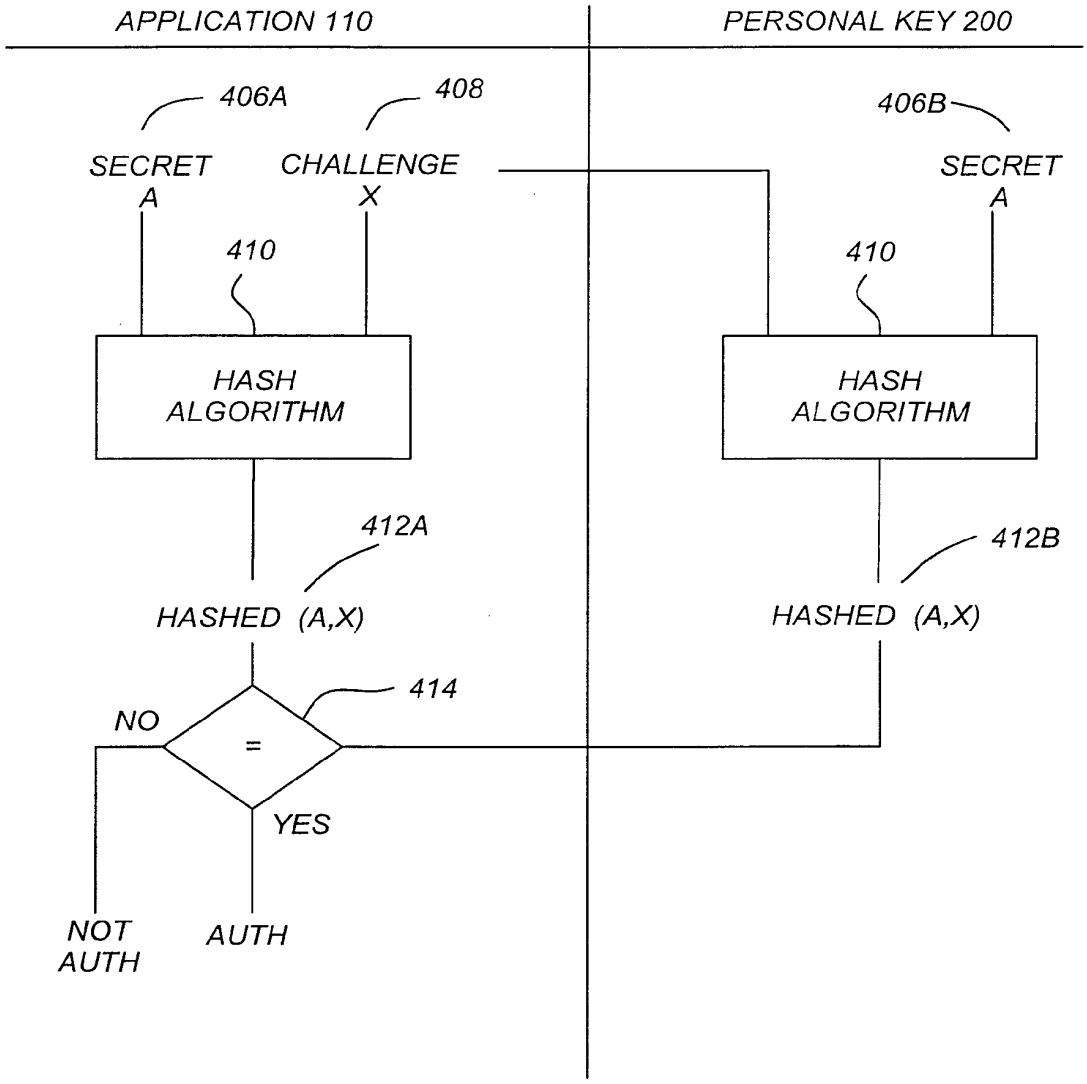

APPLICATION 110
PERSONAL KEY 200
406A
408
406B
SECRET A
CHALLENGE X
SECRET A
410
410
HASH ALGORITHM
HASH ALGORITHM
412A
412B
HASHED (A,X)
HASHED (A,X)
414
NO
=
YES
NOT AUTH
AUTH

FIG. 4

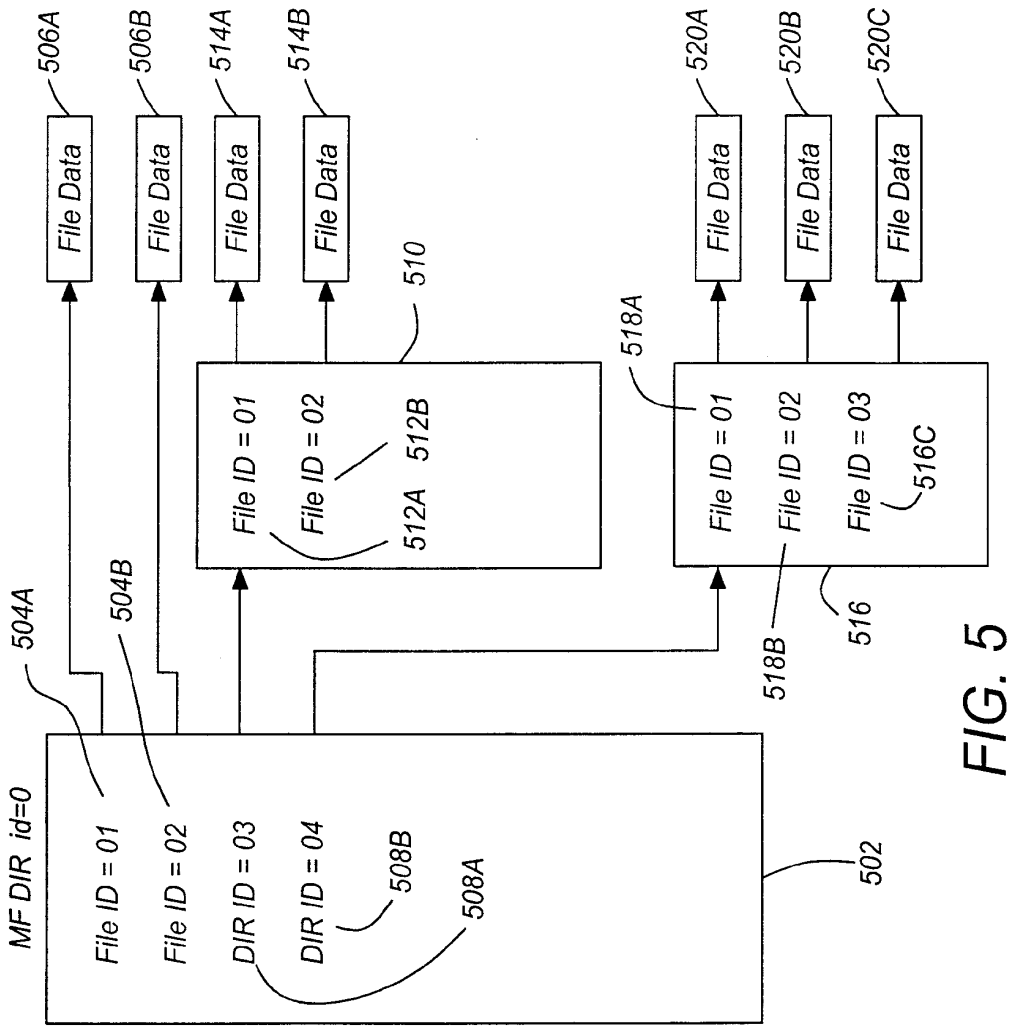

506A
506B
514A
514B
520A
520B
520C
File Data
File Data
File Data
File Data
File Data
File Data
File Data
510
518A
File ID = 01
File ID = 02
512B
512A
File ID = 01
File ID = 02
File ID = 03
516C
504A
504B
518B
516
MF DIR id=0
File ID = 01
File ID = 02
DIR ID = 03
DIR ID = 04
508B
508A
502

FIG. 5

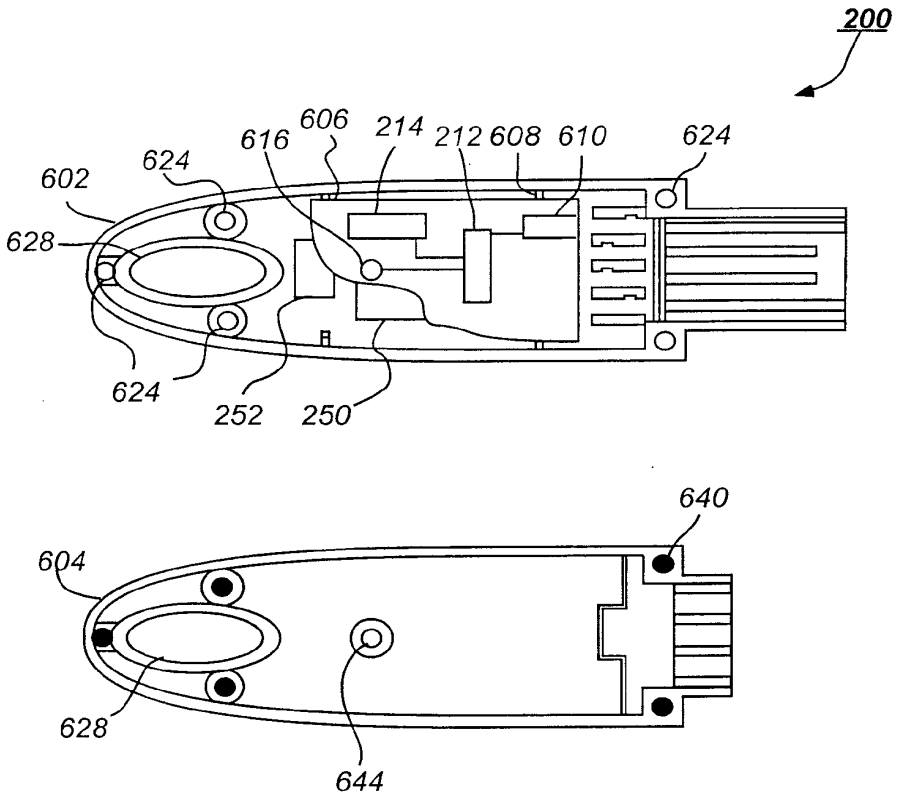

200
602
624
616
606
214
212
608
610
624
628
624
252
250
640
604
628
644

FIG. 6

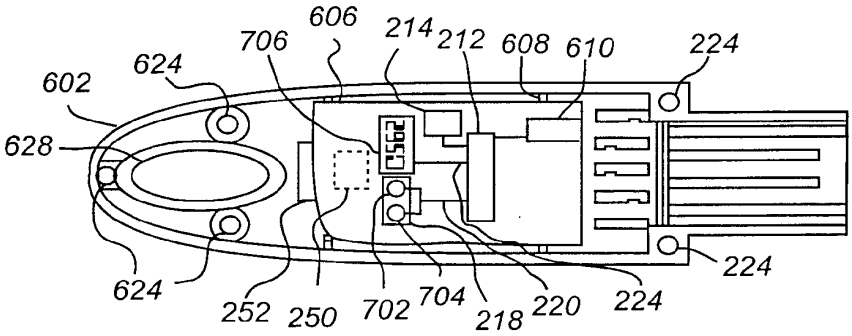


FIG. 7A

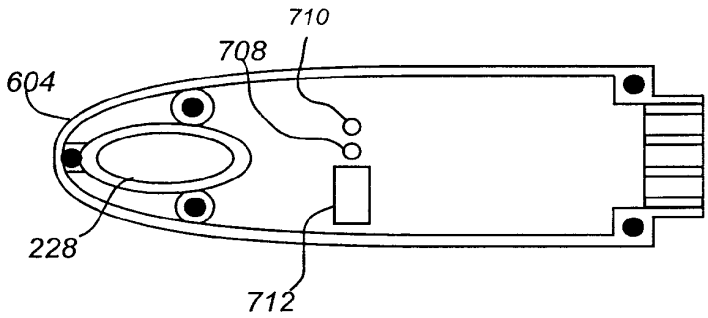


FIG. 7B

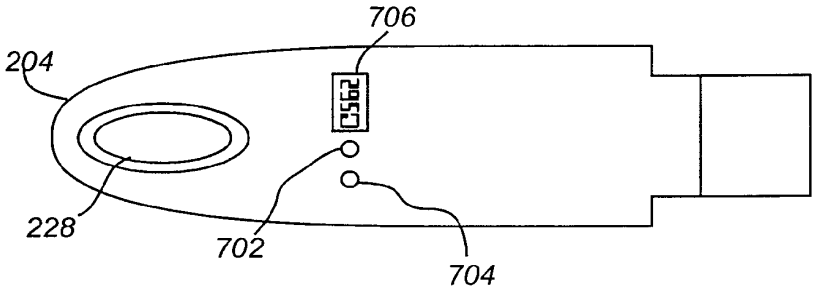


FIG. 7C

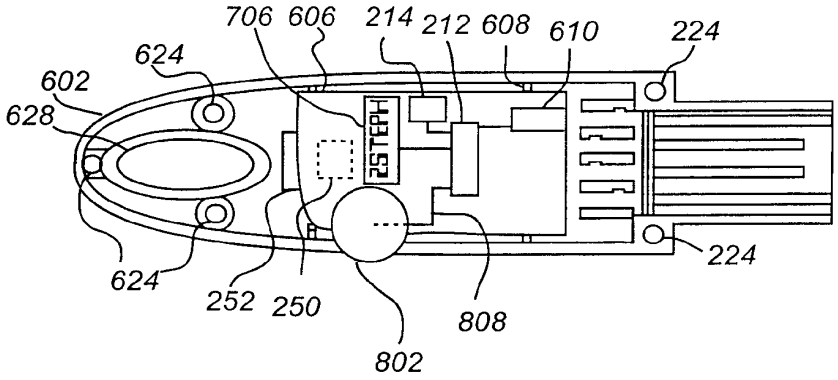


FIG. 8A

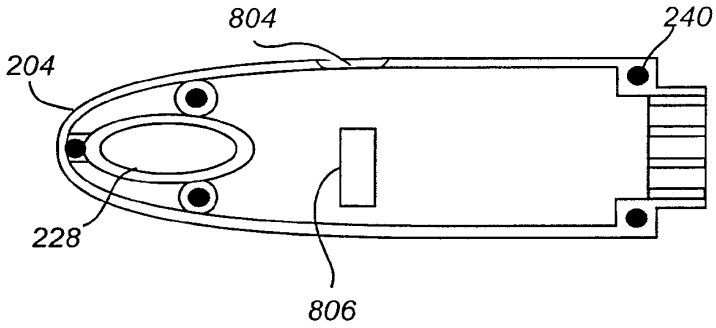


FIG. 8B

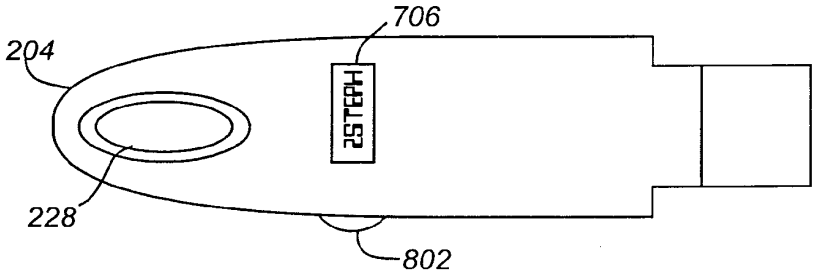


FIG. 8C

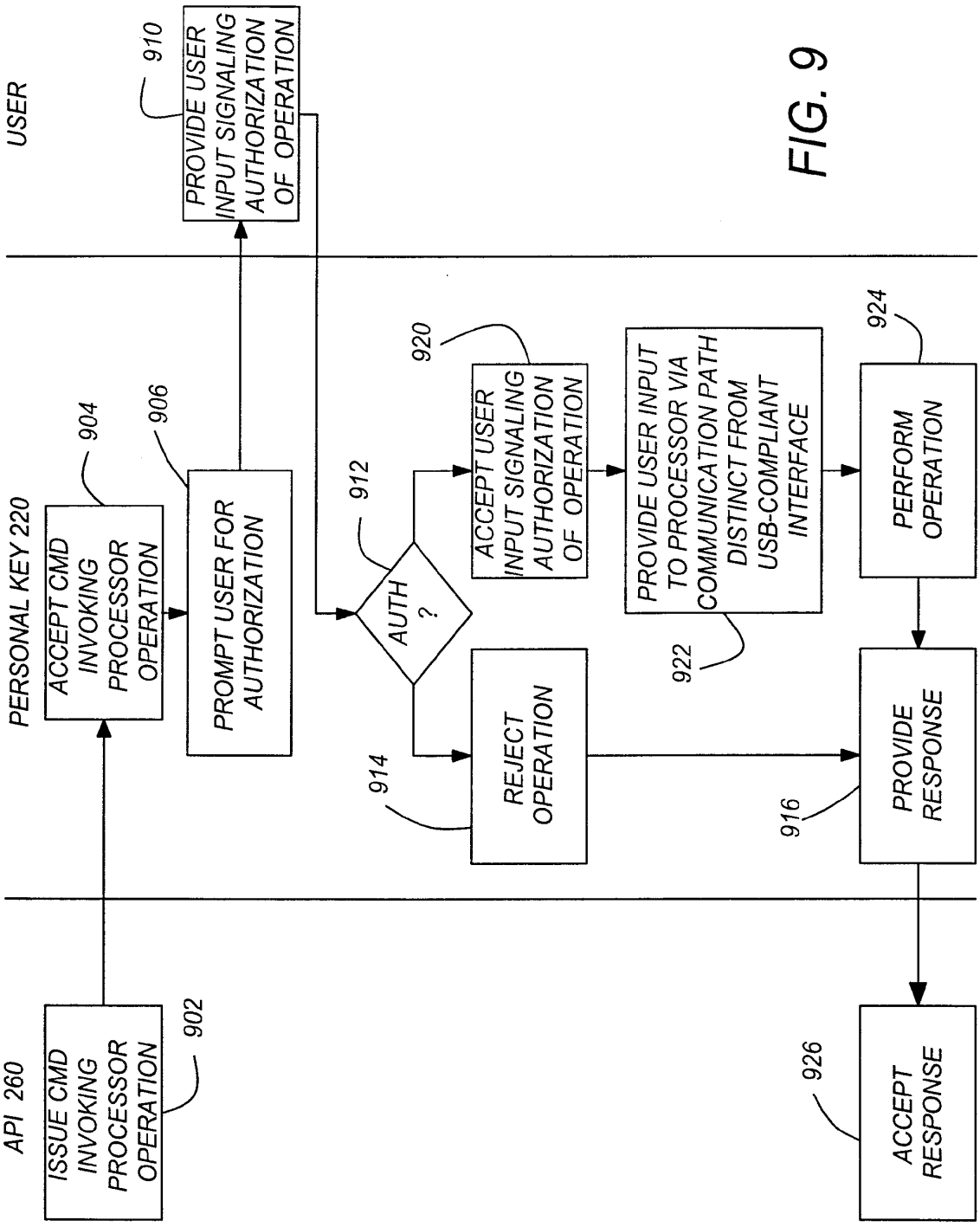

USER
PERSONAL KEY 220
API 260
ISSUE CMD INVOKING PROCESSOR OPERATION
902
ACCEPT CMD INVOKING PROCESSOR OPERATION
904
PROMPT USER FOR AUTHORIZATION
906
PROVIDE USER INPUT SIGNALING AUTHORIZATION OF OPERATION
910
AUTH ?
912
REJECT OPERATION
914
ACCEPT USER INPUT SIGNALING AUTHORIZATION OF OPERATION
920
PROVIDE USER INPUT TO PROCESSOR VIA COMMUNICATION PATH DISTINCT FROM USB-COMPLIANT INTERFACE
922
PERFORM OPERATION
924
PROVIDE RESPONSE
916
ACCEPT RESPONSE
926

FIG. 9

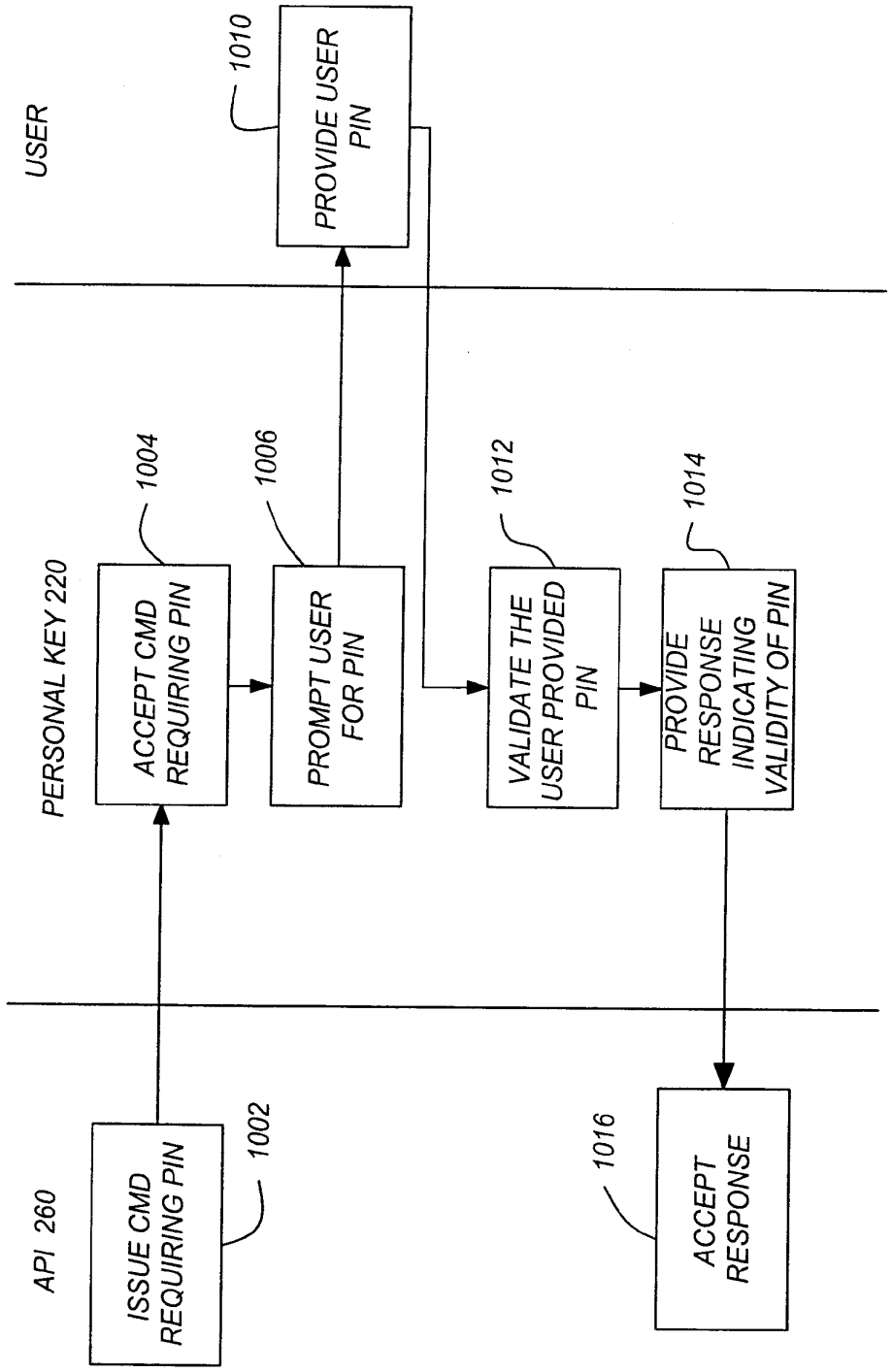

USER
PERSONAL KEY 220
API 260
PROVIDE USER PIN
1010
ACCEPT CMD REQUIRING PIN
1004
PROMPT USER FOR PIN
1006
VALIDATE THE USER PROVIDED PIN
1012
PROVIDE RESPONSE INDICATING VALIDITY OF PIN
1014
ISSUE CMD REQUIRING PIN
1002
ACCEPT RESPONSE
1016

FIG. 10

INTERNATIONAL SEARCH REPORT

Internatio. ‹pplication No
PCT/US 00/00711

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	"WIBU-KEY, User's Guide Version 2.50" 'Online! July 1998 (1998-07) , WIBU-SYSTEMS AG , KARLSRUHE, GERMANY XP002139265 Retrieved from the Internet: <URL: ftp://www2.wibu.de/pub/download/us/UG250US .pdf> 'retrieved on 2000-05-25!	1-5,7,9, 11,12, 14-16
A	page 12, paragraph 1 -page 14, paragraph 1 page 164	17

Y	GB 2 154 344 A (NAT RES DEV) 4 September 1985 (1985-09-04) page 3, line 7 - line 62; figures 1-3	1-5,7,9, 11,12, 14-16

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 May 2000	20/06/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Moens, R

1

Form PCT/ISA/210 (second sheet) (July 1992)

IPR2022-00412
Apple EX1053 Page 439

INTERNATIONAL SEARCH REPORT

Internatic Application No
PCT/US 00/00711

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 791 877 A (FRANCE TELECOM) 27 August 1997 (1997-08-27) column 3, line 43 -column 4, line 8; figures	1,3,4, 11,12,14
A	US 5 857 024 A (NISHINO KIYOSHI ET AL) 5 January 1999 (1999-01-05) column 4, line 6 - line 64; figures 1,7	1,5-9, 11-13, 15-17
A	"Rainbow Technologies Adds USB Support For PC And Macintosh Software Developers To Sentinel Line" NEWS RELEASE, 'Online! 17 November 1998 (1998-11-17), XP002139273 Retrieved from the Internet: <URL:http://www.rainbow.com/invest/PR98111 7b.html> 'retrieved on 2000-05-28! the whole document	1,3,4, 11,12,14

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

IPR2022-00412
Apple EX1053 Page 440

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internatio pplication No
PCT/US 00/00711

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2154344 A	04-09-1985	US 4799258 A	17-01-1989
EP 0791877 A	27-08-1997	FR 2745399 A	29-08-1997
US 5857024 A	05-01-1999	JP 9114946 A	02-05-1997

IPR2022-00412
Apple EX1053 Page 441

PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 : E05B 49/00

A1

(11) Internationale Veröffentlichungsnummer: WO 00/65180

(43) Internationales Veröffentlichungsdatum: 2. November 2000 (02.11.00)

(21) Internationales Aktenzeichen: PCT/EP00/02949

(22) Internationales Anmeldedatum: 3. April 2000 (03.04.00)

(30) Prioritätsdaten:
199 18 817.3 26. April 1999 (26.04.99) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: HUF HÜLSBECK & FÜRST GMBH & CO. KG [DE/DE]; Steeger Strasse 17, D–42551 Velbert (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: MÜLLER, Ulrich [DE/DE]; Schneegelskothen 7C, D–42549 Velbert (DE). VAN DEN BOOM, Andreas [DE/DE]; Mühlenkamp 35, D–45309 Essen (DE). KLEIN, Helmut [DE/DE]; Heidekamp 51, D–42549 Velbert (DE).

(74) Anwalt: MENTZEL, Norbert; Kleiner Werth 34, D–42275 Wuppertal (DE).

(81) Bestimmungsstaaten: AU, BR, CN, IN, JP, KR, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

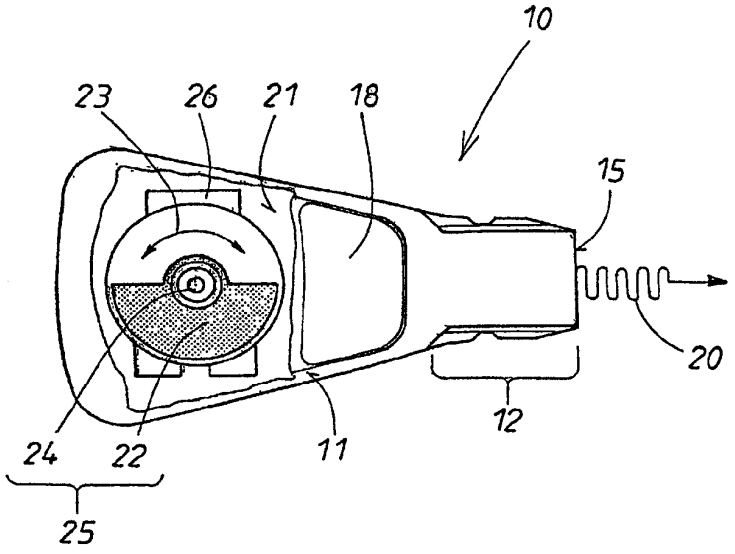
Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: ELECTRONIC KEY, IN PARTICULAR, FOR VEHICLES

(54) Bezeichnung: ELEKTRONISCHER SCHLÜSSEL, INSBESONDERE FÜR FAHRZEUGE

(57) Abstract

The invention relates to an electronic key (10), in which coded signals (20) are transmitted and optionally received. In order to achieve this, it is necessary to provide suitable electronic components which are supplied with electric energy by a current reservoir in the housing interior (21). A mass (22) is kinetically mounted (24) in the housing interior (21), in order to ensure that the electronic key (10) is continuously operational. The kinetic energy (23) of said mass (22) which is generated when the key is moved, is converted into electric energy by an electric generator (26), provided in the housing interior (21). The electric energy is subsequently used to continuously recharge the current reservoir.



(57) Zusammenfassung

Bei einem elektronischen Schlüssel (10) werden codierte Signale (20) gesendet und gegebenenfalls empfangen. Dazu sind geeignete elektronische Bauteile im Gehäuseinneren (21) notwendig, die von einem Stromspeicher mit elektrischer Energie versorgt werden. Um einen stets betriebsbereiten elektronischen Schlüssel (10) zu gewährleisten, wird vorgeschlagen, eine Masse (22) im Gehäuseinneren (21) beweglich zu lagern (24). Die beim Bewegen des Schlüssels anfallende Bewegungsenergie (23) dieser Masse (22) wird in einem im Gehäuseinneren (21) vorgesehenen elektrischen Generator (26) in elektrische Energie gewandelt, die dann zum dauernden Nachladen des Stromspeichers genutzt wird.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische Republik Mazedonien	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland			**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von Amerika
CA	Kanada	**IT**	Italien	**MX**	Mexiko		
CF	Zentralafrikanische Republik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik Korea	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun			**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

Elektronischer Schlüssel, insbesondere für Fahrzeuge

Die Erfindung richtet sich auf einen elektronischen Schlüssel der im Oberbegriff des Anspruches 1 angegebenen Art. Zum Betrieb der elektronischen Bauteile verwendet man in der Regel elektrische Batterien in Form von sogenannten Knopfzellen. Nach einiger Gebrauchszeit entleeren sich die Batterien. Es müssen daher Vorkehrungen getroffen werden, um die Batterien bequem ausbauen, neue Batterien wieder einbauen und zuverlässig kontaktieren zu können. Dafür muss ein geeigneter Platz im Schlüsselgehäuse reserviert sein. Das ist aufwendig. Das Auswechseln der Batterie ist mühevoll und erfordert eine eingehende Belehrung des Schlüsselbesitzers, der dazu nicht immer bereit ist.

Man kann anstelle von solchen Einweg-Batterien auch Akkumulatoren als Stromspeicher für die elektrische Energie im Schlüsselgehäuse verwenden. Es sind aber zum regelmäßigen Aufladen eines solchen Stromspeichers Anschlüsse im Schlüsselgehäuse erforderlich, deren Anordnung wegen der sehr begrenzten Gehäuseoberfläche problematisch ist. Außerdem sind Anzeigemittel für den Ladezustand des Stromspeichers erforderlich, wenn man von einer plötzlichen Entleerung des Stromspeichers nicht überrascht werden will. Auch das erfordert an der Gehäuseoberfläche Platz. Vor allem ist aber während des Ladevorgangs der Schlüssel nicht nutzbar. Der Schlüsselinhaber muss daher die Pausen zwischen der Benutzung des Schlüssels nutzen und die Ladetätigkeit gut einplanen. Das wird als störend empfunden.

IPR2022-00412
Apple EX1053 Page 444

Für den Betrieb elektrischer Kleingeräte (DE 196 20 880 A1) ist es bekannt, die zum bestimmungsgemäßen Gebrauch des Geräts erforderliche manuelle Betätigung eines Funktionsauslöseelements dazu zu verwenden, um daraus eine elektrische Energie zu gewinnen. Als Kleingerät verwendete man dabei auch einen mechanischen Schlüssel mit integrierter Infrarot-Sendeeinrichtung. Weil zur Gewinnung der elektrischen Energie ein entsprechendes, mechanisches Energieäquivalent aufgebracht werden muss, ist der Betätiger bei diesem Kleingerät schwergängig. Dies wirkt sich unangenehm bei der Handhabung aus.

Bei einem Türschloss mit einem manuell mittels eines Schlüssels schließbaren Schlossriegel (DE 32 08 818 C2) verwendete man einen elektrischen Antrieb für den Schlossriegel. Der elektrische Antrieb war an einen netzunabhängigen Speicher oder Generator angeschlossen. Die bestimmungsgemäße Betätigung des Schlosses beim Öffnen und Schließen wurde dazu genutzt, um den Generator anzutreiben. Die Betätigung zur Gewinnung elektrischer Energie konnte in einem Fall vom Türgriff ausgehen, der mit dem Generator gekuppelt war. In einem anderen Fall war das Antriebsritzel des dynamischen Generators mit einer Zahnstange eines im Schloss längsverschieblichen Schlüssels verbunden, der beim Ein- bzw. Ausstecken über den Generator elektrische Energie erzeugte.

Schließlich ist es bekannt (DE 197 21 001 C1) bei einem elektronischen Gerät einen längsverschieblichen Schieber oder einen drehbaren Rotationskörper vorzusehen, der, um elektrische Energie für das Gerät zu gewinnen, mit der Hand oder mit den Fingern bewegt werden musste. Die elektrische Energie wurde hier zwar auf mechanischem Wege erzeugt, doch musste dazu der Schieber bzw. der Rotationskörper gezielt manuell angetrieben werden. Das war mühsam und zeitaufwendig. Wurde es vergessen lag keine nutzbare elektrische Energie vor, weshalb der Betrieb des elektronischen Geräts ausfiel. Der Schieber bzw. der Rotationskörper erfordert einen großen Flächenbereich auf der Gehäuseaußenseite, um für die Hand zu Antriebszwecken gut zugänglich zu sein. Die Anwendung auf elektronische Schlösser war zwar vorgesehen, ist aber für elektronische Schlüssel ungeeignet.

IPR2022-00412
Apple EX1053 Page 445

Es ist bei Armbanduhren bekannt, dreh- oder schwenkbewegliche Pendel im Uhrengehäuse vorzusehen, welche für die mechanische Energieversorgung des Uhrwerks sorgen. Es liegt aber nicht nahe diese Uhrenmechanik auf elektronische Schlüssel zu übertragen, die, abgesehen von einem eventuellen mechanischen Notschlüssel, keine mechanische Funktionen haben und auf einen elektrischen Stromspeicher angewiesen sind.

Der Erfindung liegt die Aufgabe zugrunde einen preiswerten elektronischen Schlüssel der im Oberbegriff des Anspruches 1 genannten Art zu entwickeln, dessen Betriebsbereitschaft sich durch einen besonders bequemen Service auszeichnet. Dies wird erfindungsgemäß durch die im Kennzeichen des Anspruches 1 angeführten Maßnahmen erreicht, denen folgende besondere Bedeutung zukommt.

Die Erfindung hat erkannt, dass der elektronische Schlüssel normalerweise Bewegungen ausgesetzt ist, die sich in Beschleunigungen und Verzögerungen des Schlüssels auswirken. Dadurch werden unvermeidlich dauernd mechanische Kräfte auf den Schlüssel ausgeübt, die zur Gewinnung von mechanischer Energie genutzt werden können. Dies tritt nicht nur in einer Ruhephase des Schlüssels ein, wenn der Schlüssel vom Besitzer in der Hosentasche od. dgl. getragen wird und der Schlüsselbesitzer sich bewegt, sondern auch während der Arbeitsphase des Schlüssels, wenn der Schlüssel im Schloss steckt und das Fahrzeug sich beschleunigend oder verzögernd bewegt.

Ordnet man nun eine Masse im Schlüsselgehäuse beweglich an, so kann die dort anfallende mechanische Energie von einem elektrischen Generator in elektrische Energie gewandelt werden. Diese elektrische Energie kann dann zum Aufladen des im Schlossgehäuse befindlichen Stromspeichers genutzt werden.

Bei der Erfindung ist nicht nur der Stromspeicher sondern auch die Aufladeeinrichtung und die Energieerzeugung im Inneren des Schlüsselgehäuses integriert. Es brauchen daher an der Gehäuseoberfläche keinen besonderen Maßnahmen zur Zugänglichkeit ins Schlüsselinnere oder zur Energieversorgung von

IPR2022-00412
Apple EX1053 Page 446

außen erfolgen. Der Schlüsselinhaber braucht sich um die Energieversorgung des elektronischen Schlüssels überhaupt nicht mehr zu kümmern; das Aufladen des Schlüssels erfolgt automatisch bei jeder Schlüsselbewegung, also sowohl in der Ruhe- als auch in der Gebrauchsphase des Schlüssels. Der erfindungsgemäße Schlüssel ist stets betriebsbereit.

Weitere Maßnahmen und Vorteile der Erfindung ergeben sich aus dem Unteranspruch, der nachfolgenden Beschreibung und der Zeichnung. In der Zeichnung ist die Erfindung schematisch in einem Ausführungsbeispiel dargestellt. Es zeigen:

Fig. 1 die Seitenansicht eines elektronischen Schlüssels mit einem Gehäuseausbruch und

Fig. 2 ein Blockschaltbild zur Verdeutlichung des inneren Aufbaus und der Wirkungsweise des erfindungsgemäßen Schlüssels.

Der elektronische Schlüssel 10 umfasst ein Schlüsselgehäuse 11 dessen eines Ende 12 mit einem geeigneten Einsteckprofil 12 versehen ist. Diesem elektronischen Schlüssel ist ein komplementäres elektronisches Schloss zugeordnet, das eine geeignete Aufnahme für das Einsteckprofil 12 aufweist. Im Schlüsselinneren sind verschiedenste elektronische Bauteile 13 vorgesehen, die in definierter Weise miteinander geschaltet sind, z.B. über Leiterbahnen einer sogenannten elektrischen Leiterplatte. Die elektronischen Bauteile 13 haben verschiedene Funktionen zu erfüllen. Außer der Kommunikation mit dem zugehörigen Schloss gehört dazu auch das Aussenden oder Empfangen von codierten Signalen 20, z.B. in Form einer elektromagnetischen hochfrequenten Strahlung. Dazu ist ein geeigneter Sender 14 im Schlüsselgehäuse integriert, zweckmäßigerweise am Stirnende 15 des Einsteckabschnitts 12.

Zur Energieversorgung der Schaltung und ihrer Bauteile 13 dient ein elektrischer Stromspeicher 16. Die elektrischen Bauteile 13 können durch einen Schalter 17

IPR2022-00412
Apple EX1053 Page 447

wirksam gesetzt werden. Der Schalter 17 wird von einem Betätiger 18, z.B. einem Taster, ein- und/oder ausgeschaltet. Das ist durch einen Betätigungspfeil 19 im Schema von Fig. 2 veranschaulicht. Dieser Betätiger 18 ist durch eine geeignete Profilierung eines Gehäusebereichs in die Gehäuseschale integriert.

Im Gehäuseinneren 21 ist eine Masse 22 beweglich gelagert, wie durch den Bewegungspfeil 23 veranschaulicht ist. Im vorliegenden Fall ist diese Masse 22 an einem Lagerzapfen 24 frei drehgelagert, weshalb hier ein Pendel 25 vorliegt. Diese Pendelbewegung 25 wird als mechanische Energie einem zugeordneten Generator 26 zugeführt, der elektrische Energie erzeugt und diese über die in Fig. 2 verdeutlichte elektrische Verbindung 27 zum Aufladen des Stromspeichers 16 nutzt.

Die rotatorische Energie eines Pendels 25 ist zwar besonders geeignet, doch wäre es auch möglich, die mechanische Energie durch eine translatorische Bewegung einer Masse 22 zu erzeugen. Die mechanische Energie kann in beliebiger Weise durch bewegliche Massen oder Flüssigkeiten im Inneren des Schlüsselgehäuses erzeugt werden. Entscheidend ist, dass die bei der Benutzung und Nichtbenutzung des Schlüssels anfallenden mechanischen Bewegungen in elektrische Energie umgewandelt werden, die zur Versorgung der elektronischen Bauteile beim bestimmungsgemäßen Gebrauch des elektronischen Schlüssels dient.

IPR2022-00412
Apple EX1053 Page 448

Bezugszeichenliste :

10	elektronischer Schlüssel
11	Schlüsselgehäuse von 10
12	Einsteckprofil von 11, Einsteckbereich
13	elektronische Bauteile in 11
14	Sender in 11
15	Stirnende von 12
16	Stromspeicher in 11
17	Schalter
18	Betätiger, Taster
19	Betätigungspfeil von 18
20	codiertes Signal von 14
21	Gehäuseinneres von 11
22	freibewegliche Masse
23	Bewegungspfeil von 22, Pendelbewegung
24	Lagerzapfen von 22
25	Pendel aus 22, 24
26	Generator
27	elektrische Verbindung zwischen 26, 16

IPR2022-00412
Apple EX1053 Page 449

Patentansprüche :

1.) Elektronischer Schlüssel (10), insbesondere für Fahrzeuge, mit einem Schlüsselgehäuse (11), beinhaltend

einen Sender (14) und gegebenenfalls einen Empfänger für codierte Signale (20) zwecks Kommunikation mit einem zugehörigen elektronischen Schloss,

eine elektrische Schaltung mit elektronischen Bauteilen (13) zur Generierung, zur Codierung und gegebenenfalls zur Decodierung der Signale (20)

und einen Stromspeicher (16) für die zum Betrieb der elektronischen Bauteile (13) benötigte elektrische Energie,

dadurch gekennzeichnet ,

dass eine bewegliche (23) Masse (22) im Schlüsselgehäuse (11) angeordnet ist und beim Bewegen des Schlüssels mechanische Energie erzeugt,

dass im Schlüsselgehäuse (11) ein Wandler, wie ein elektrischer Generator (26), angeordnet ist, der die mechanische Energie in elektrische Energie wandelt,

und dass die elektrische Energie zum Aufladen des Stromspeichers (16) im Schlüsselgehäuse (11) dient.

2.) Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass die bewegliche Masse (22) aus einem schwenk- bzw. drehgelagerten (24) Pendel (25) besteht.

IPR2022-00412
Apple EX1053 Page 450

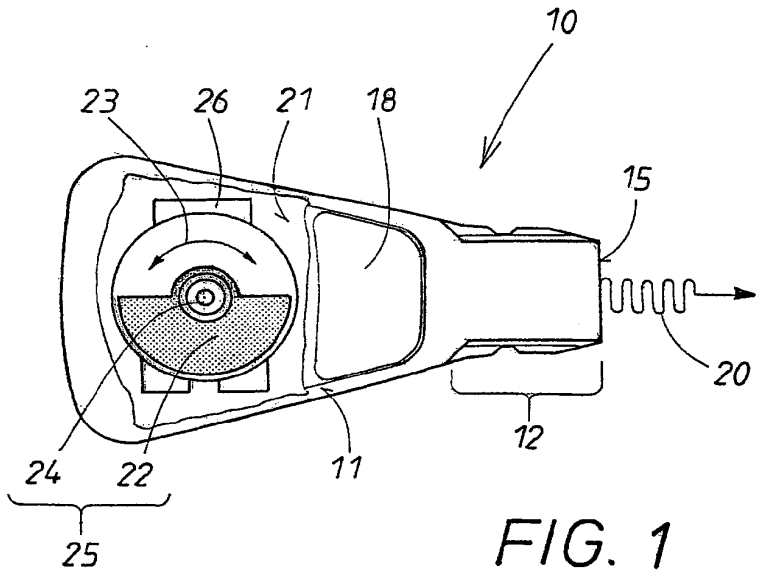


FIG. 1

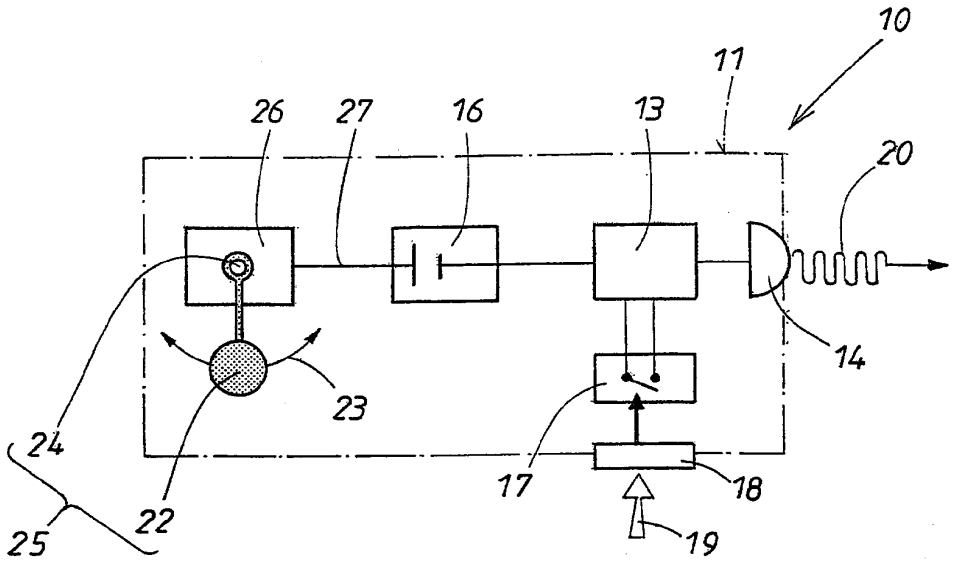


FIG. 2

IPR2022-00412
Apple EX1053 Page 451

INTERNATIONAL SEARCH REPORT

Inte. ..ional Application No
PCT/EP 00/02949

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 E05B49/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 E05B G04C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	DE 196 20 880 A (BRANDESTINI) 27 November 1997 (1997-11-27) cited in the application the whole document	1,2
Y	WO 84 01041 A (KNAPEN) 15 March 1984 (1984-03-15) abstract	1,2
A	EP 0 170 303 A (KINETRON BV) 5 February 1986 (1986-02-05) abstract	1,2
A	FR 2 407 599 A (JUILLET) 25 May 1979 (1979-05-25) the whole document	1,2

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 August 2000	24/08/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Van Beurden, J

Form PCT/ISA/210 (second sheet) (July 1992)

IPR2022-00412
Apple EX1053 Page 452

INTERNATIONAL SEARCH REPORT

Inte. ional Application No
PCT/EP 00/02949

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19620880 A	27-11-1997	CN 1219298 A	09-06-1999
		WO 9744883 A	27-11-1997
		EP 0900467 A	10-03-1999
WO 8401041 A	15-03-1984	NL 8203443 A	02-04-1984
		AU 1944983 A	29-03-1984
		EP 0119223 A	26-09-1984
EP 0170303 A	05-02-1986	NL 8402113 A	03-02-1986
		AT 40223 T	15-02-1989
		DE 3567750 D	23-02-1989
		JP 1612218 C	30-07-1991
		JP 2035547 B	10-08-1990
		JP 61018326 A	27-01-1986
		KR 9005809 B	11-08-1990
		US 4644246 A	17-02-1987
FR 2407599 A	25-05-1979	NONE	

Form PCT/ISA/210 (patent family annex) (July 1992)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 00/02949

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 E05B49/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 E05B G04C

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, PAJ, WPI Data

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	DE 196 20 880 A (BRANDESTINI) 27. November 1997 (1997-11-27) in der Anmeldung erwähnt das ganze Dokument	1,2
Y	WO 84 01041 A (KNAPEN) 15. März 1984 (1984-03-15) Zusammenfassung	1,2
A	EP 0 170 303 A (KINETRON BV) 5. Februar 1986 (1986-02-05) Zusammenfassung	1,2
A	FR 2 407 599 A (JUILLET) 25. Mai 1979 (1979-05-25) das ganze Dokument	1,2

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
10. August 2000	24/08/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Van Beurden, J

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

IPR2022-00412
Apple EX1053 Page 454

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 00/02949

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 19620880 A	27-11-1997	CN 1219298 A	09-06-1999
		WO 9744883 A	27-11-1997
		EP 0900467 A	10-03-1999
WO 8401041 A	15-03-1984	NL 8203443 A	02-04-1984
		AU 1944983 A	29-03-1984
		EP 0119223 A	26-09-1984
EP 0170303 A	05-02-1986	NL 8402113 A	03-02-1986
		AT 40223 T	15-02-1989
		DE 3567750 D	23-02-1989
		JP 1612218 C	30-07-1991
		JP 2035547 B	10-08-1990
		JP 61018326 A	27-01-1986
		KR 9005809 B	11-08-1990
		US 4644246 A	17-02-1987
FR 2407599 A	25-05-1979	KEINE	

IPR2022-00412
Apple EX1053 Page 455

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 December 2000 (14.12.2000)

PCT

(10) International Publication Number
WO 00/75755 A1

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/IT00/00216

(22) International Filing Date: 25 May 2000 (25.05.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
TO99A000480 8 June 1999 (08.06.1999) IT

(71) Applicant *(for all designated States except US)*: **EUTRON INFOSECURITY S.R.L.** [IT/IT]; Via Gandhi, 12, I-24048 Curnasco di Treviolo (IT).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LEIDI, Michele** [IT/IT]; Eutron Infosecurity S.r.l., Via Gandhi, 12, I-24048 Curnasco di Treviolo (IT). **CASSIA, Lucio** [IT/IT]; Eutron Infosecurity S.r.l., Via Gandhi, 12, I-24048 Curnasco di Treviolo (IT).

(74) Agent: **GARAVELLI, Paolo**; A.Bre.Mar. S.r.l., Via Servais, 27, I-10146 Torino (IT).

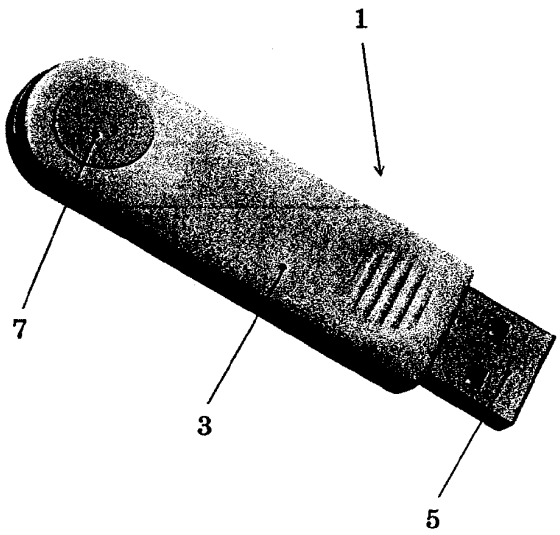
(81) Designated States *(national)*: AE, AL, AU, BA, BB, BG, BR, CA, CN, CR, CU, CZ, DM, EE, GD, GE, HR, HU, ID, IL, IN, IS, JP, KP, KR, LC, LK, LR, LT, LV, MA, MG, MK, MN, MX, NO, NZ, PL, RO, SG, SI, SK, TR, TT, UA, US, UZ, VN, YU, ZA.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*
— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: IDENTIFICATION DEVICE FOR AUTHENTICATING A USER



(57) Abstract: A device (1) is described to authenticate a user in an Internet environment, comprising: a support structure (3); a terminal (5) for the connection to a processor port; a microprocessor circuitry to perform safety functions and cryptography algorithms; and activation means (7) to allow enabling an authentication code. A system and a process are further described to input a PIN inside the device (1) and a system and a process to authenticate a user based on such device (1).

WO 00/75755 A1

IDENTIFICATION DEVICE FOR AUTHENTICATING A USER

The present invention refers to a user authentication system within an Internet architecture based on an hardware device connected to the Universal Serial Bus (USB) port of a client processor through a cryptographic procedure of the "Challenge Response" type. Moreover, the invention refers to a hardware and software system to input a Personal Identification Number (PIN) inside the above-said identification device based on USB port in order to prevent the interception thereof.

With the always wider spreading of the Internet network and other networks of this type, a particular and major importance has been given to problems about the controlled distribution of information on the network, in order to guarantee that these information cannot be attacked and guarantee their privacy as well, in addition to

IPR2022-00412
Apple EX1053 Page 457

providing access to particular transactions or information only to authorised users. Several arrangements have so far been proposed, starting from the so-called protecting "hardware keys" to be connected to processors, up to more or less complex cryptographic systems with different types of software keys. The proposed solutions either are very costly to be implemented in terms of several types of resources, or do not guarantee a complete safety of the information to be protected.

Object of the present invention is solving the above prior-art problems, by providing an hardware and software system that is of a reduced cost, easily implemented and absolutely efficient in terms of protection. In particular, the hardware device of the invention is of a simple configuration, has the sizes of a key and, once being inserted into the USB port of a computer, allows univocally recognising and authenticating the user of a network-based application and to start therewith protected and encrypted transactions on the Internet network itself. Authentication uniqueness and transaction safety are based on the features of the device, that is equipped with a microprocessor implemented for

IPR2022-00412
Apple EX1053 Page 458

safety functions, and on private-key time-varying cryptographic algorithms.

The above and other objects and advantages of the invention, as will appear from the following description, are obtained by a user authentication device and process as claimed in Claims 1 and 6, respectively, and by a system and process that use the above device as claimed in Claims 15 and 17, respectively. Preferred embodiments and non-trivial variations of the present invention are claimed in the dependent Claims.

The present invention will be better described by some preferred embodiments thereof, given as a non-limiting example, with reference to the enclosed drawings, in which:

- Figure 1 is a perspective view of an embodiment of the device according to the present invention;
- Figure 2 is a block diagram of the architecture of the code-inputting system of the device of the invention;
- Figure 3 is a block diagram of the process realised by the architecture in Fig. 2;
- Figure 4 is a block diagram detailing a step of the process in Fig. 3;

IPR2022-00412
Apple EX1053 Page 459

- Figure 5 is a block diagram detailing a step of the process in Fig. 3;
- Figure 6 is a block diagram of the operating process of the device in Fig. 1;
- Figure 7 is a block diagram detailing a step of the process in Fig. 6;
- Figure 8 is a block diagram detailing a step of the process in Fig. 6;
- Figure 9 is a block diagram summarising the steps of the processes in Fig.s 7 and 8; and
- Figure 10 is a block diagram detailing a step of the process in Fig. 6.

With reference to Fig. 1, the device 1 for authenticating a user in an Internet architecture environment substantially comprises an elongated support structure 3, preferably made of plastic material and adapted to be grasped by a user and inserted into a port of a client processor (not shown), for example the Universal Serial Bus (USB) port of a personal computer. For such purpose, the device 1 is equipped with a terminal 5 for the connection to the port and with a microprocessor circuitry contained inside the support structure 3; the circuitry is adapted to perform safety

IPR2022-00412
Apple EX1053 Page 460

functions and to operate on cryptographic algorithms. Finally, the device 1 of the invention comprises activation means 7 (commonly realised in the shape of a push-button) supported by the structure 3 and adapted to control the microprocessor circuitry to allow enabling therein an authentication code, as will be described hereinbelow.

In the current and preferred embodiment, the device 1 operates on cryptographic algorithms that are of the private-key time-varying type. Due to the standard interface and "plug&play" USB and to a set of interfacing libraries of the ActiveX and Plug-In type on server and client sides, the device 1 is efficient in terms not only of safety, but also of simplicity and transparency. Its features make it an efficient tool to store keywords, electronic certificates, digital signatures, electronic purse functions or to store and protect therein other interesting information related to user or used services.

With the device 1 of the invention, those who need protecting and checking the access to pages, services, data bases or more generally to areas of Internet sites, will simply have to supply

IPR2022-00412
Apple EX1053 Page 461

authorised users of their one Internet service with a suitably initialised device 1. The users will then have to simply insert the device 1 into the USB port of the computer without performing any installation operation. The server application will take care of setting a safe communication with the device 1 in order to authenticate the user. User recognition in fact occurs depending on reserved information inside the device linked with a user keyword. Once having recognised the client and having checked affected user authorisations, the device 1 takes care of sending customised and reserved information to the user, encrypting the contents with an algorithm of the 256-bit Blowfish type, for example, with a time-varying key linked to the secret value contained into the device 1. Information can be indifferently, but not in a limiting way, HTML pages, data bases information with "web" interface, forms, download areas, and the like. The information transaction of the network is performed encrypted both from server to client, and vice versa.

In order to be able to use the above-described device 1, it is necessary to equip it with a univocal Personal Identification Number (PIN) per

IPR2022-00412
Apple EX1053 Page 462

user. For such purpose, a system has been implemented whose architecture is shown in Fig. 2, such system being adapted to perform a process as detailed in Figures 3 to 5.

With reference first of all to Fig. 2, the system architecture that allows using the device 1 substantially comprises a processor equipped with a graphic window 10 that displays a digit from 0 to 9. Such window cooperates with a user library 12 (arrow A in Fig. 2), that is a proprietary library that deals with managing the device 1 and, through an identification process 14 contained therein, with checking the enabling of the device 1 itself.

The user library 12 is connected (arrow B in Fig. 2) with a device driver 16, that is also a proprietary library that deals with managing the device 1 at USB level. The device driver 16 is connected (arrow C in Fig. 2) with the device 1 that receives commands (arrow D in Fig. 2) from the push-button 7. According to the flow defined by arrows A to D, in the user library 12 an internal tick pulse is generated so that, upon every tick, a digit is sent both to the window 10 for being displayed, and to the device 1 through the device driver 16; the device driver 16 queries the device

IPR2022-00412
Apple EX1053 Page 463

1 whether there are other digits and, if the response is affirmative, goes on with the processing, while otherwise it warns the user library 12 to stop the process. Upon every pressure of the push-button 7, the device 1 stores the currently supplied digit that is also displayed by the window 10.

The general operation of the above-described system is shown as a block diagram in Fig.s 3 to 5. Such process guarantees the maximum safety when inputting the PIN to use the device 1. The process first of all comprises, upon request of the PIN code, the activation (301) of the graphic window 10 to display a current digit from 0 to 9.

Then the PIN code is sent (303) for every digit, through a process inserted into the libraries, both to the displaying window 10 and to the device 1.

Upon pressing the push-button 7, therefore, every digit is stored (305) as belonging to the PIN code; then, the process that sends the digit both to the graphic window 10 and to the device 1, queries (307) every time the device 1 to check whether there are other digits: if the response is affirmative, the process goes on by timely sending

IPR2022-00412
Apple EX1053 Page 464

(309) the other digits; otherwise, it stops (311) and the final PIN key is stored to validate the device 1.

Upon a more detailed examination, the operation of the PIN code storing step (305) can be divided into two major steps, where the first one deals with managing the display and dispatch of the digits to the device 1, while the second one deals with managing the push-button 7 of the device 1 itself.

In particular, as shown in detail in Fig. 4, the displaying and dispatching step of the digits to the device 1 starts in 401 and comprises the following sub-steps:

- creating (403) the window 10 to display the digits;
- querying (405) whether the digits limit has been reached;
- in case of an affirmative response, removing (407) the displaying window 10; or
- in case of a negative response, sending (409) the digit to the graphic window 10 and to the device 1; and
- requesting (411) to the device 1 whether the

IPR2022-00412
Apple EX1053 Page 465

digits limit for the PIN code has been reached, returning to the querying step (405): if the response is affirmative, the process finally ends in 413.

With reference to Fig. 5, instead, the flow diagram of the management step for the push-button 7 of the device 1 is shown in detail, this step being able to be divided into the following sub-steps, starting from the initial one in 501:

- querying (503) whether the digits limit has been reached;
- in case of an affirmative response, ending (509) the process; or
- in case of a negative response, checking (505) whether the push-button 7 has been pressed;
- in case of a negative response, the procedure remains waiting for a following pressure of the push-button 7; or
- in case of an affirmative response, storing (507) the last received digit and returning to the querying step (503) are performed.

After having defined the device 1 of the invention in this way and the system and process to

IPR2022-00412
Apple EX1053 Page 466

store and validate the personal code inside the device, it is possible to practice the real and proper process of the invention to manage the accesses to reserved pages and services being present on the Internet network.

As already stated, the system that allows such process is composed, preferably but not in a limiting way, of a central server processor (not shown) that stores and manages the authorised users, connected to a set of local client processors (not shown) equipped with the device 1 of the invention. The detailed procedure is commonly realised through programs being present on both server and client processors, and is shown in Fig.s 7 to 10 of the description.

In particular, with reference to Fig. 6, the process for authenticating a user in an Internet architecture environment comprises the following macro-steps:

- associating (601) a user with an identification device 1;
- identifying (603) the user through the device 1; and
- encrypting (605) information sent/received by/from the user.

IPR2022-00412
Apple EX1053 Page 467

In particular, as shown in Fig. 7, the associating step (601) of a user to the device 1 comprises the following sub-steps:

- describing (701) the user;
- generating (703) a TokenId based on describing data of the user;
- performing (705) a first irreversible safe scrambling step (preferably of the MD5 type) of the TokenId after a communication (709) with the server processor managing the keywords;
- creating (706) a first Personal Identification Number (PIN) from the first scrambling (705);
- performing (707) a second irreversible safe scrambling step (preferably of the MD5 + 3DES type) of the TokenId after a communication (709) with the server processor for the keywords;
- creating (708) a second Personal Identification Number (PIN2) from the second scrambling (705), where the second Personal Identification Number (PIN2) is different from the first Personal Identification Number

IPR2022-00412
Apple EX1053 Page 468

(PIN);

- associating the user with an identification string composed of the TokenId, the first Personal Identification Number (PIN) and the second Personal Identification Number (PIN2); and
- storing such complete identification string into the device 1 and the TokenId alone into a data base on the server processor.

With reference now to Fig. 8 in particular and to Fig. 9 as assembly view of the two steps shown in Fig.s 7 and 8, the user identifying step (603) through the device 1 is shown in detail; it comprises the following sub-steps:

- in case of an access by the user to web pages of the network in which an access control must be performed, the server processor sends (801) to the client processor a string of the "Server Challenge" type, that is always different; the string is associated with the first Personal Identification Number (from 706) and is processed by the client to be able to provide a response for the server. For this purpose, the process proceeds with the steps of:

IPR2022-00412
Apple EX1053 Page 469

- performing (803) an hashing step (preferably of the MD5 type) on the "Server Challenge" string and the first Personal Identification Number, thereby producing (805) a text string;
- using (807) the second Personal Identification Number (PIN2) (from 708) as encrypting key of a cryptography (809) (preferably of the 3DES type) on the text string;
- generating (811, 813) a string comprising the TokenId and a Response Client and sending such string to the server processor;
- comparing (step 901 in Fig. 9) on the server the received string with the Response Client being generated on the server side by re-processing the first and second Personal Identification Numbers (PIN, PIN2); and
- in case of a positive response to such comparing step (901), pointing out (step 903 in Fig. 9) the existence of a correct identification code; or
- in case of a negative response to such comparing step (901), pointing out (step 905

IPR2022-00412
Apple EX1053 Page 470

in Fig. 9) the existence of an incorrect or counterfeited identification code.

Finally, with reference to Fig. 10, the information encrypting step (605) comprises the following sub-steps, performed by the server processor:

- generating (1000) an encryption key from the previous encrypting step (809) by using as input the Server Challenge string and the first and second Personal Identification Numbers (PIN, PIN2);
- receiving (1003) a page from the network;
- encrypting (1001) (preferably using the Blowfish encryption) the received page through the generated encryption key; and
- sending (1005) the encrypted page to the client processor, which, once having received the encrypted pages, is able to decrypt them and reproduce them in a clear way, because it knows both the Server Challenge string and the first and second Personal Identification Numbers (PIN, PIN2).

Some embodiments of the invention have been described, but obviously they are subjected to further modifications and variations within the

IPR2022-00412
Apple EX1053 Page 471

same inventive idea. For example, several construction variations of the device 1 will be possible, both from the point of view of the connections to external processor ports, and from the point of view of the internal circuitry to realise the described functionalities. Moreover, the various processes of the invention could be applied to various types of authentication devices, and the systems to realise the described processes could be implemented according to different connection configurations to various types of networks.

IPR2022-00412
Apple EX1053 Page 472

CLAIMS

1. Device (1) for authenticating a user in an Internet architecture environment, characterised in that the device comprises:

- a support structure (3);
- a terminal (5) for the connection to a port of a processor;
- a microprocessor circuitry contained inside said support structure (3), said circuitry being adapted to perform safety functions and operating on cryptographic algorithms; and
- activation means (7) supported by said structure (3) and adapted to control said microprocessor circuitry to allow enabling therein an authentication code.

2. Device (1) according to Claim 1, characterised in that said terminal (5) is adapted to be connected to a port of the Universal Serial Bus (USB) type of a personal computer.

3. Device (1) according to Claim 1, characterised in that said activation means (7) are composed of a push-button.

IPR2022-00412
Apple EX1053 Page 473

4. Device (1) according to Claim 1, characterised in that said cryptographic algorithms performed by said microprocessor circuitry are of the private-key time-varying type.

5. Device (1) according to Claim 3, characterised in that said cryptographic algorithms are of the "Challenge Response" type.

6. Process for authenticating a user in an Internet architecture environment, characterised in that the process comprises the following steps:

- associating (601) a user with an identification device (1);
- identifying (603) said user through said device (1); and
- encrypting (605) information sent/received by/from said user.

7. Process according to Claim 6, characterised in that said device (1) is the device according to any one of Claims 1 to 5.

8. Process according to Claim 6, characterised in that said associating step (601) comprises the following sub-steps:

IPR2022-00412
Apple EX1053 Page 474

- describing (701) said user;
- generating (703) a TokenId based on describing data of said user;
- performing (705) a first irreversible safe scrambling step of said TokenId after a communication (709) with a keywords server processor;
- creating (706) a first Personal Identification Number (PIN) from said first scrambling (705);
- performing (707) a second irreversible safe scrambling step of said TokenId after a communication (709) with a keywords server processor, said second scrambling (707) being different from said first scrambling (705);
- creating (708) a second Personal Identification Number (PIN2) from said second scrambling (705), said second Personal Identification Number (PIN2) being different from said first Personal Identification Number (PIN);
- associating said user with an identification string composed of said TokenId, said first Personal Identification Number (PIN) and said

IPR2022-00412
Apple EX1053 Page 475

second Personal Identification Number (PIN2); and

- storing said complete identification string into said device (1) and said TokenId into a data base on said server processor.

9. Process according to Claim 8, characterised in that said first scrambling (705) is of the MD5 type and said second scrambling (707) is of the MD5 + 3DES type.

10. Process according to any one of Claims 6 to 9, characterised in that said identifying step (603) comprises the following sub-steps:

- in case of an access by said user to pages of said network in which an access control must be performed, sending (801) by the server processor a string of the "Server Challenge" type, said string being associated with said first Personal Identification Number;
- performing (803) an hashing step on said "Server Challenge" string and said first Personal Identification Number, thereby producing (805) a text string;
- using (807) said second Personal Identification Number (PIN2) as encrypting

IPR2022-00412
Apple EX1053 Page 476

key of a cryptography (809) on said text string;

- generating (811, 813) a string comprising said TokenId and a Response Client and sending said string to said server processor;
- comparing (901) said received Response Client string with the Response Client being generated on the server side by re-processing said first and second Personal Identification Numbers (PIN, PIN2); and
- in case of a positive response to said comparing step (901), pointing out (903) the existence of a correct identification code; or
- in case of a negative response to said comparing step (901), pointing out (905) the existence of an incorrect or counterfeited identification code.

11. Process according to Claim 10, characterised in that said hashing is of the MD5 type and said cryptography (809) is of the 3DES type.

12. Process according to any one of Claims 6 to 11, characterised in that said encrypting step (605) comprises the following sub-steps, performed by said server processor:

IPR2022-00412
Apple EX1053 Page 477

- generating (1000) an encryption key from said encrypting step (809) by using as input said Server Challenge string and said first and second Personal Identification Numbers (PIN, PIN2);
- receiving (1003) a page of said network;
- encrypting (1001) said received page through said generated encryption key; and
- sending (1005) said encrypted page to said client processor, said client processor being able to perform the decrypting of said encrypted page depending on said Server Challenge string and said first and second Personal Identification Numbers (PIN, PIN2) being known thereto.

13. Process according to Claim 12, characterised in that said encrypting (1001) is of the Blowfish type.

14. System for authenticating a user in an Internet architecture environment, characterised in that the system comprises:

- at least one central management server processor connected in a network;
- at least one local client processor connected

IPR2022-00412
Apple EX1053 Page 478

in the network;

- at least one authentication device (1) according to any one of Claims 1 to 5 connected to said at least one local client processor; and
- a control program adapted to perform the process according to any one of Claims 6 to 13.

15. System for inputting a Personal Identification Number (PIN) code inside an identification device (1) in order to prevent intercepting said device (1), characterised in that the system comprises, connected to said device (1), a processor containing:

- at least one user library (12) for managing said device (1), said user library (12) being equipped with an identification process (14) adapted to control the enabling of said device (1);
- at least one device driver (16) connected to said user library (12), said device driver (16) being a library that manages said device (1) at connection port level; and

IPR2022-00412
Apple EX1053 Page 479

- at least one window (10) connected to said user library (12) to display said PIN code digit by digit.

16. System according to Claim 15, characterised in that said device (1) is the device according to any one of Claims 1 to 5.

17. Process for inputting a Personal Identification Number (PIN) code inside an identification device (1) in order to prevent intercepting said device (1), characterised in that the process comprises the following steps:

- upon request of said PIN code, activating (301) a graphic window (10) to display an current digit from 0 to 9;
- sending (303) every digit of said PIN code both to the displaying window (10) and to the device (1);
- in case of actuation of activation means (7) of said device (1), storing (305) every digit as belonging to said PIN code;
- querying (307) said device (1) to check whether other digits exist;
- in case of an affirmative response to said

IPR2022-00412
Apple EX1053 Page 480

querying step (307), timely sending (309) the other digits; or

- in case of a negative response to said querying step (307), stopping (311) the process and storing the final PIN key to validate said device (1).

18. Process according to Claim 17, characterised in that said PIN code storing step (309) comprises the following steps:

- displaying and dispatching the digits to said device (1); and
- managing the activation means (7) of said device (1).

19. Process according to Claim 18, characterised in that said displaying and dispatching step of the digits to said device (1) comprises the following sub-steps:

- creating (403) a window (10) to display the digits;
- querying (405) whether the digits limit has been reached;
- in case of an affirmative response to said querying step (405), removing (407) said displaying window (10); or

IPR2022-00412
Apple EX1053 Page 481

- in case of a negative response to said querying step (405), sending (409) the digit to said graphic window (10) and to said device (1); and
- requesting (411) to said device (1) whether the digits limit for the PIN code has been reached, returning to said querying step (405).

20. Process according to Claim 18, characterised in that said managing step of the activation means (7) of said device (1) comprises the following sub-steps:

- querying (503) whether the digits limit has been reached;
- in case of an affirmative response to said querying step (503), ending (509) said process; or
- in case of a negative response to said querying step (503), checking (505) whether said activation means (7) are actuated;
- in case of a negative response to said checking step (505), suspending the procedure that remains in stand-by; or
- in case of an affirmative response to said

IPR2022-00412
Apple EX1053 Page 482

checking step (505), storing (507) the last received digit and returning to said querying step (503).

21. Process according to Claim 17, characterised in that said device (1) is the device according to any one of Claims 1 to 5.

IPR2022-00412
Apple EX1053 Page 483

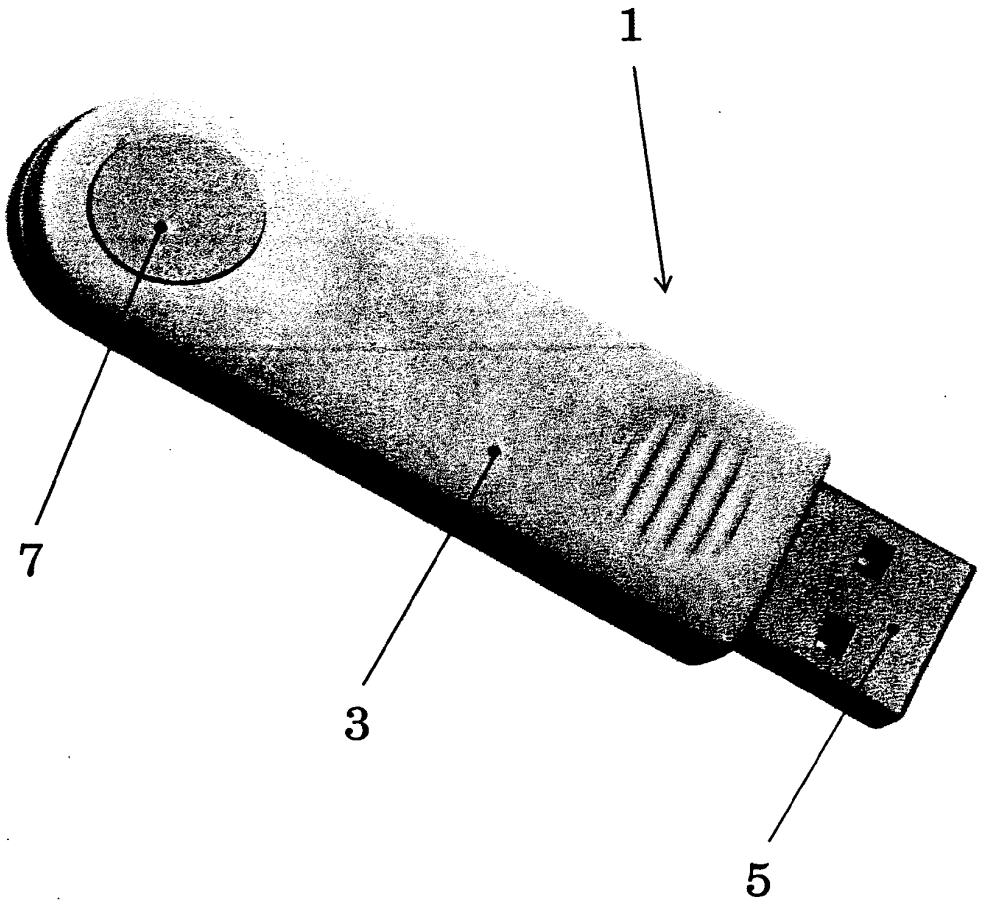


Fig. 1

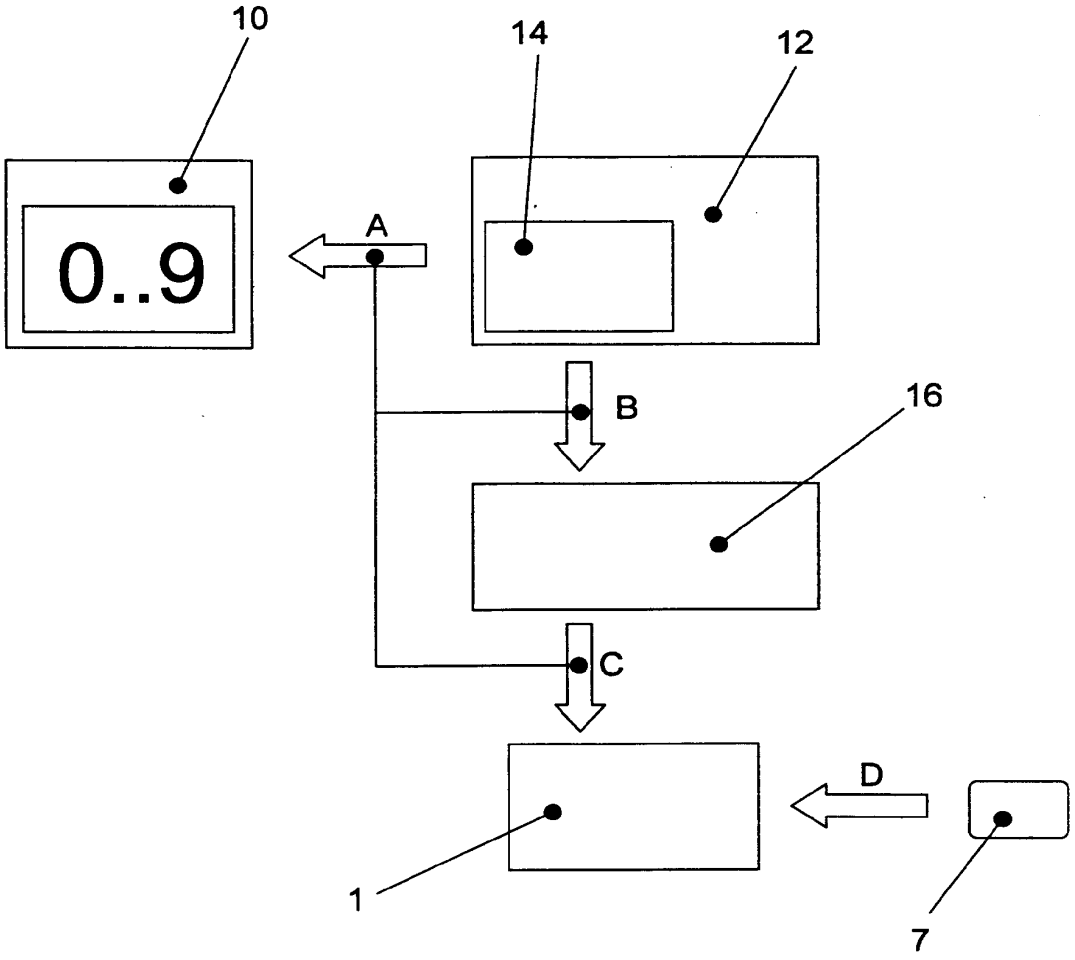


FIG. 2

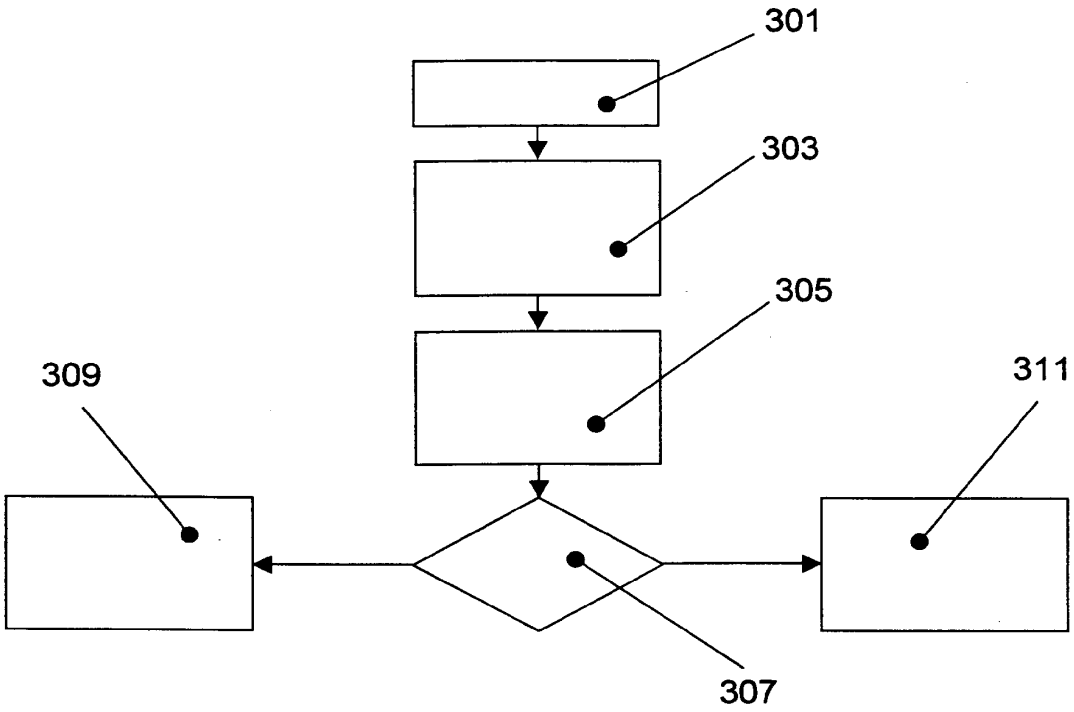


FIG. 3

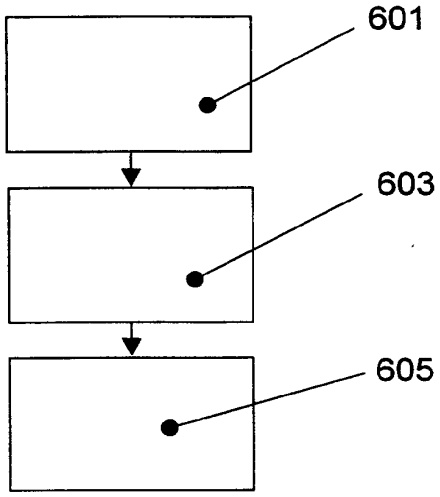


FIG. 6

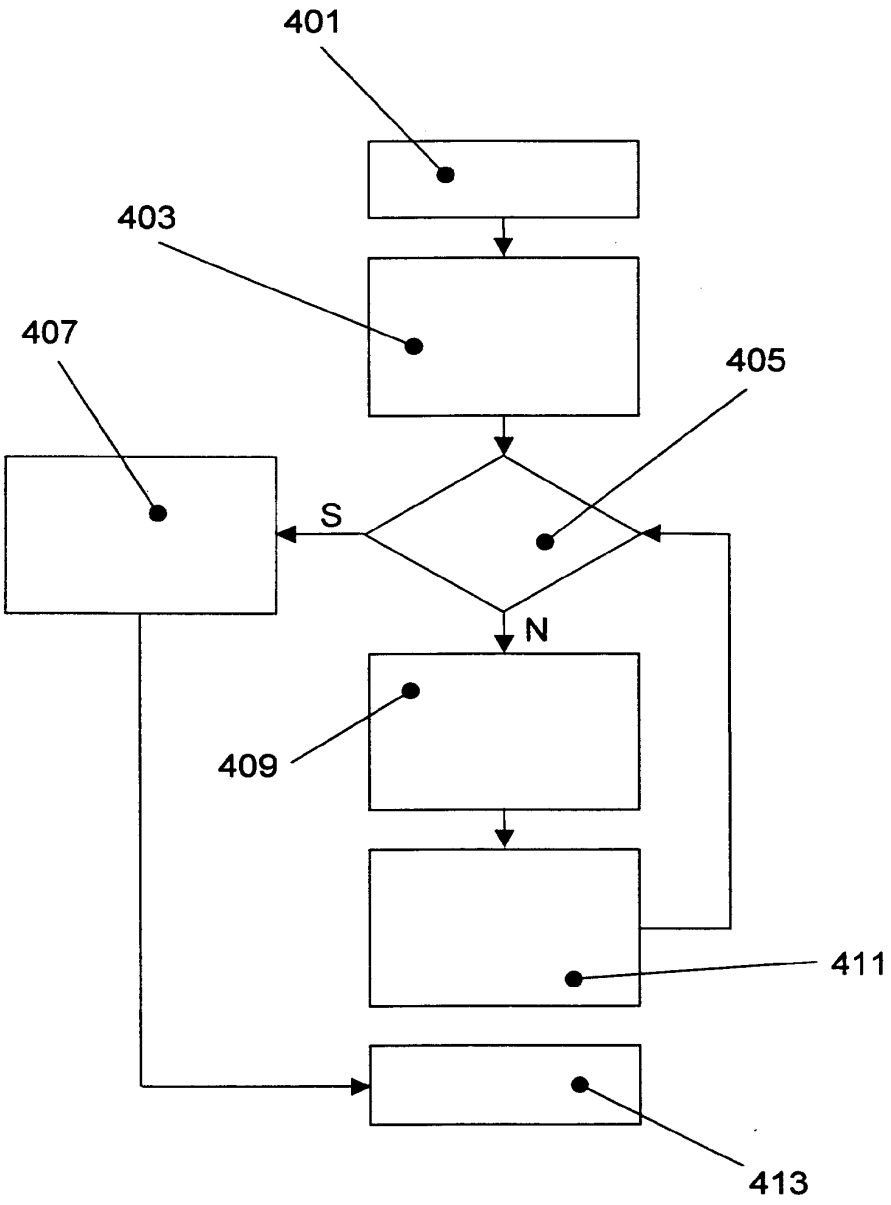


FIG. 4

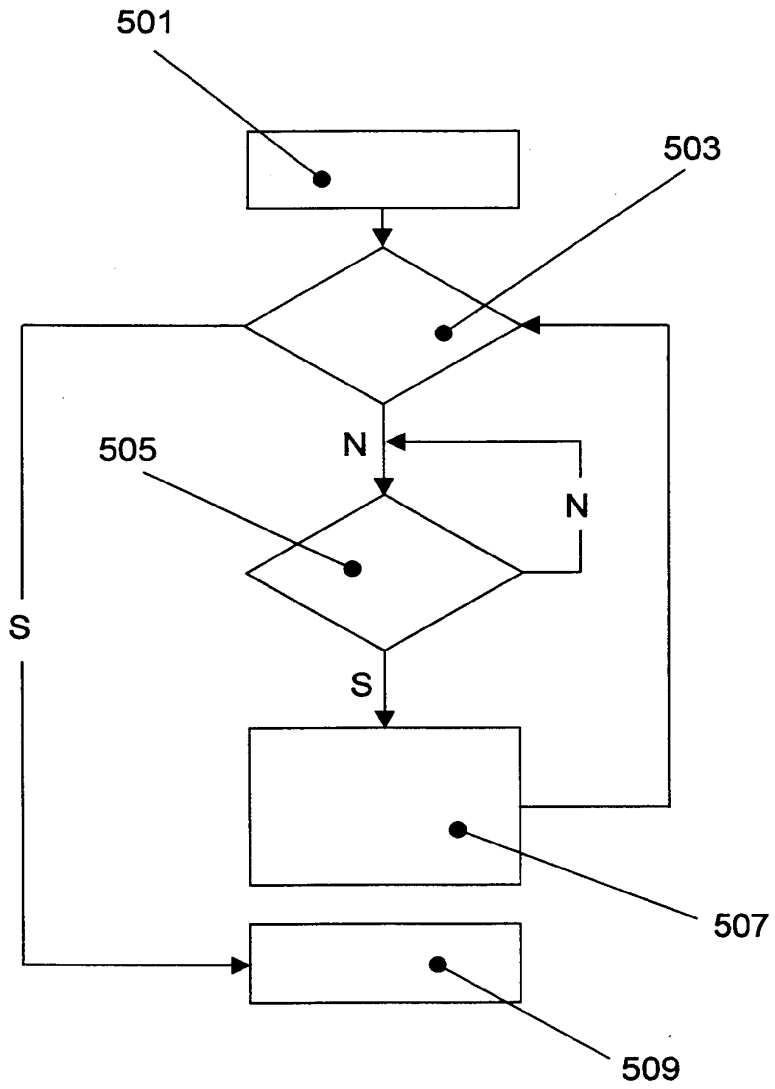


FIG. 5

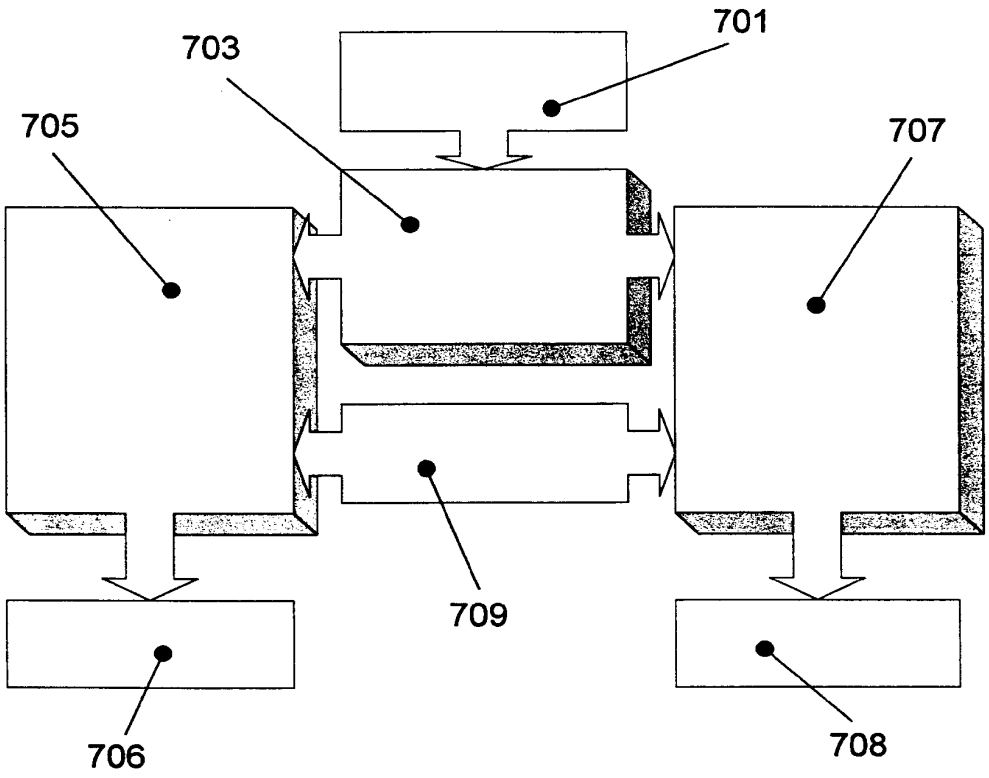


FIG. 7

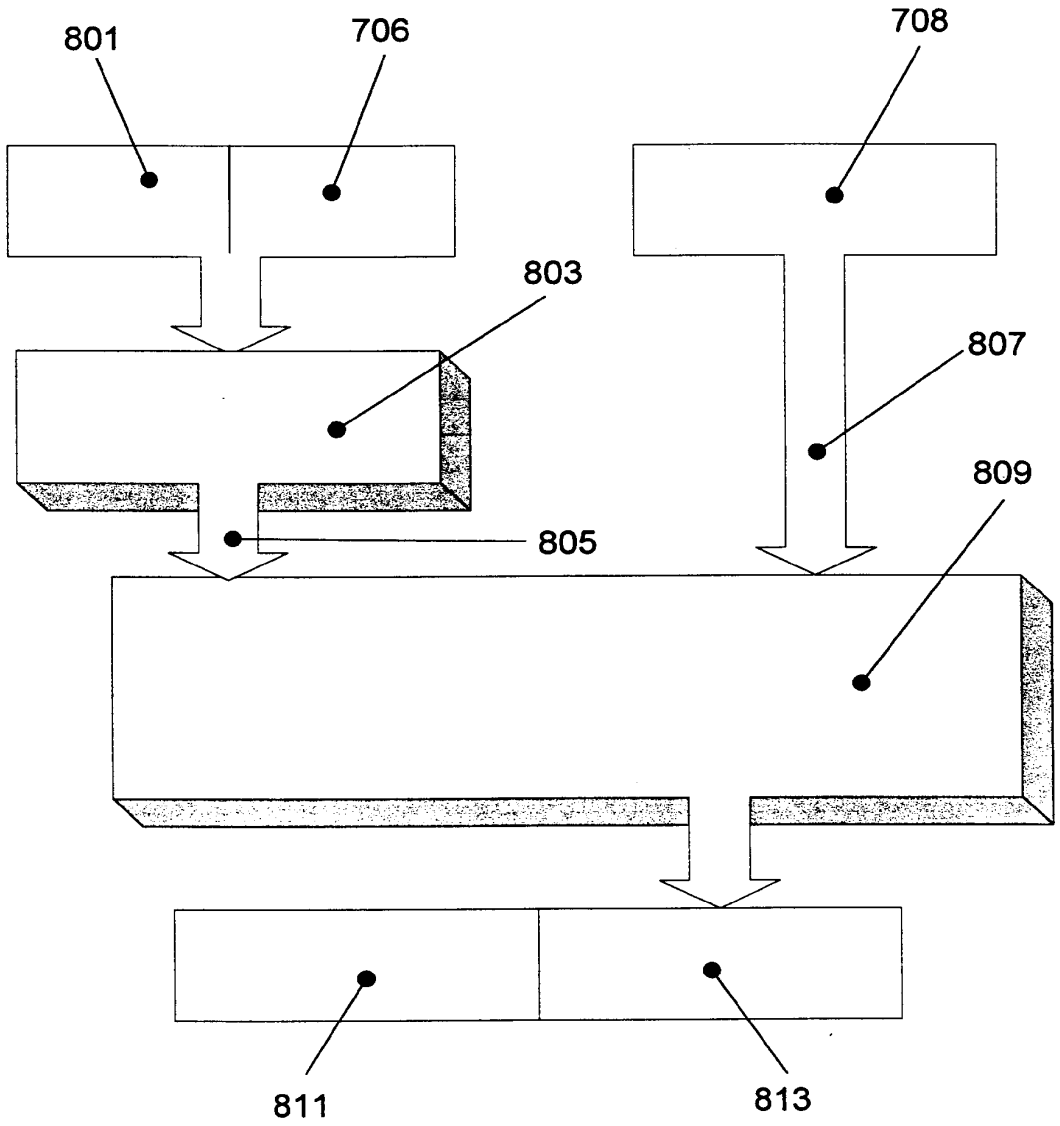


FIG. 8

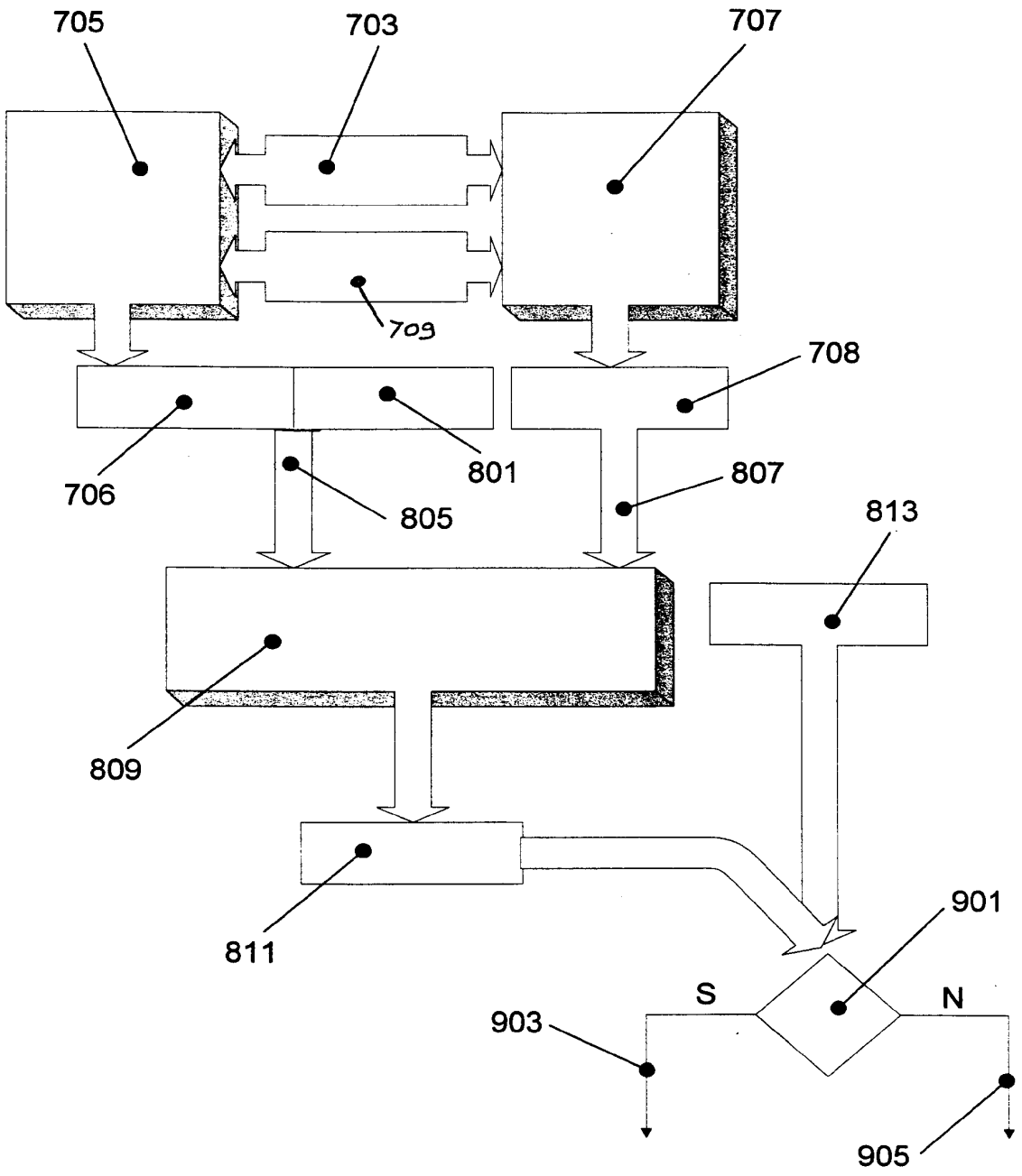


FIG. 9

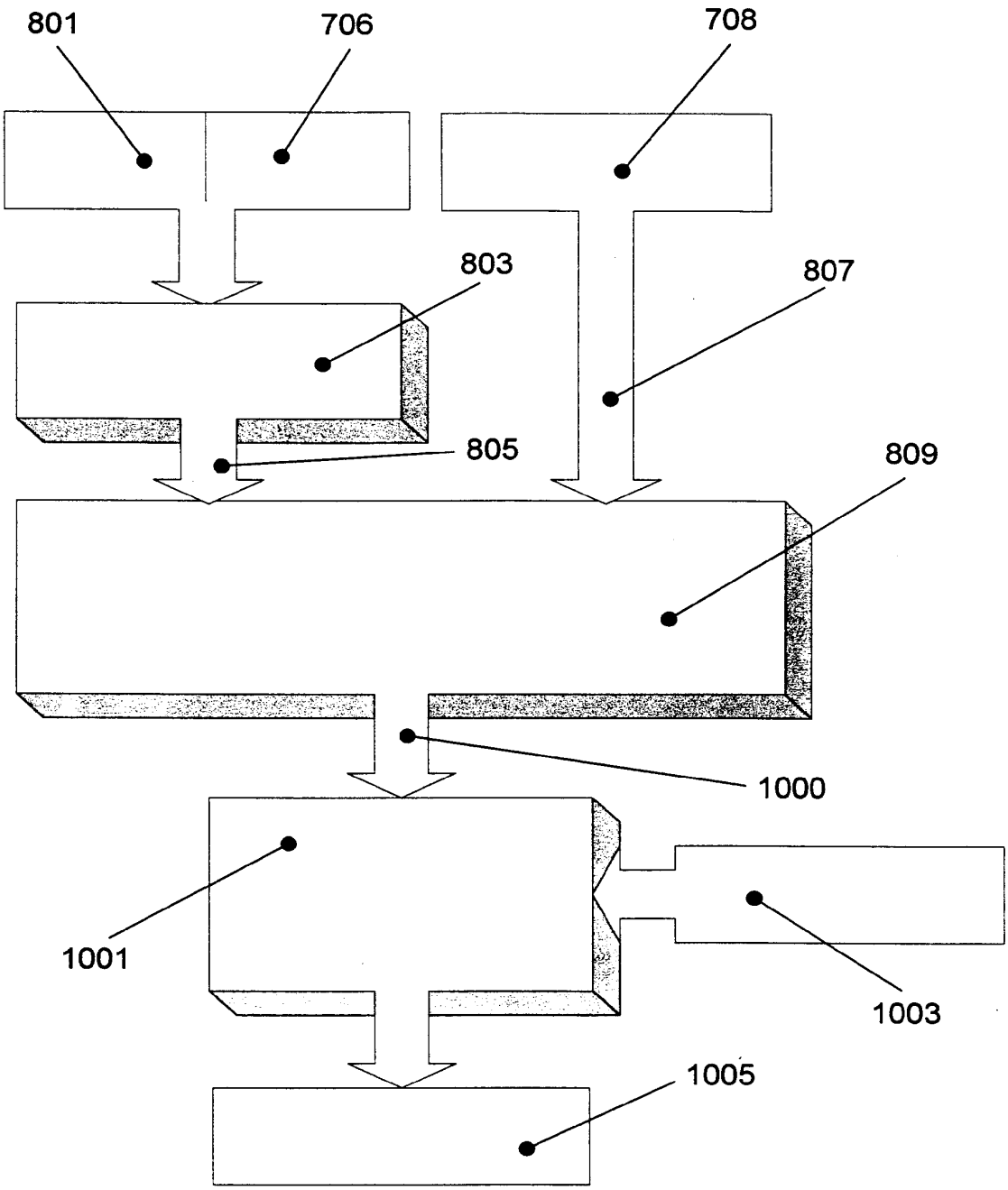


FIG. 10

INTERNATIONAL SEARCH REPORT

Int' ional Application No
PCT/IT 00/00216

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	US 5 778 071 A (CAPUTO ET AL) 7 July 1998 (1998-07-07) column 7, line 21 - line 36 column 10, line 51 -column 12, line 22 column 13, line 4 -column 18, line 9; figures 1D,2,4,5-8 ---	1,3-7,14 8-13, 15-21
A	L. PREUSS: "Rainbow Technologies Adds USB Support For PC And Macintosh Software Developers To Sentinel Line" NEWS RELEASE, 17 November 1998 (1998-11-17), XP002139273 the whole document --- -/--	1,2,4-7, 14,15,17

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 October 2000	02/11/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Moens, R

2

Form PCT/ISA/210 (second sheet) (July 1992)

IPR2022-00412
Apple EX1053 Page 493

INTERNATIONAL SEARCH REPORT

Int tional Application No
PCT/IT 00/00216

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 060 263 A (BOSEN ROBERT J ET AL) 22 October 1991 (1991-10-22) column 4, line 6 -column 5, line 24	15,17
E	WO 00 42491 A (RAINBOW TECHNOLOGIES INC) 20 July 2000 (2000-07-20) page 16, line 16 - line 20; claims 1-3,5,6; figures 7,8	1-5

2

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

IPR2022-00412
Apple EX1053 Page 494

INTERNATIONAL SEARCH REPORT

Information on patent family members

Lite ional Application No
PCT/IT 00/00216

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5778071 A	07-07-1998	US 5546463 A	13-08-1996
		AU 4147097 A	06-03-1998
		EP 0916210 A	19-05-1999
		WO 9807255 A	19-02-1998
		US 5878142 A	02-03-1999
US 5060263 A	22-10-1991	NONE	
WO 0042491 A	20-07-2000	NONE	

Form PCT/ISA/210 (patent family annex) (July 1992)

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
1. März 2001 (01.03.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/14179 A1

(51) Internationale Patentklassifikation[7]: B60R 25/04

(21) Internationales Aktenzeichen: PCT/EP00/07769

(22) Internationales Anmeldedatum:
10. August 2000 (10.08.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 39 733.3 21. August 1999 (21.08.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **HUF HÜLSBECK & FÜRST GMBH & CO. KG** [DE/DE]; Steeger Strasse 17, 42551 Velbert (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **WITTWER, Reinhard** [DE/DE]; Beuthener Strasse 26, 42579 Heiligenhaus (DE). **BARRENBERG, Günter** [DE/DE]; Am Buschkothen 20, 42551 Velbert (DE).

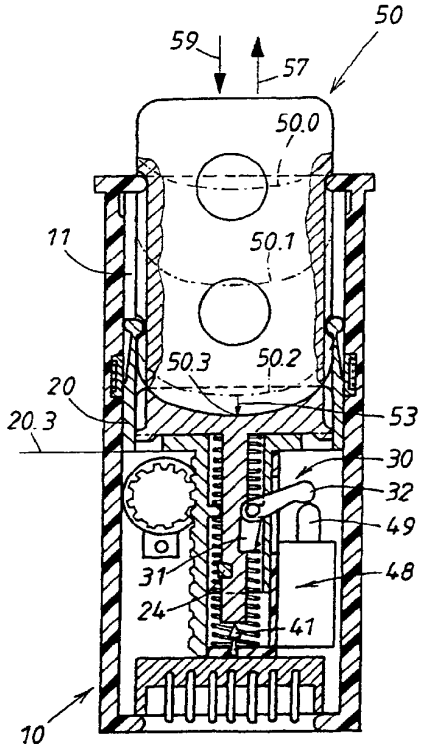
(74) Anwalt: **MENTZEL, Norbert**; Kleiner Werth 34, 42275 Wuppertal (DE).

(81) Bestimmungsstaaten *(national)*: AU, BR, CN, IN, JP, KR, US.

[Fortsetzung auf der nächsten Seite]

(54) Title: DEVICE FOR STARTING A MOTOR VEHICLE MOTOR, USING AN ELECTRONIC KEY

(54) Bezeichnung: VORRICHTUNG ZUM STARTEN EINES FAHRZEUGMOTORS MITTELS EINES ELEKTRONISCHEN SCHLÜSSELS



(57) Abstract: The invention relates to a device for starting a motor vehicle motor. According to the invention, a slot is (11) used for inserting (59) the key (50) which is usually closed by a spring-loaded cover (14). The key (50) is displaced in the slot (11) into various key positions (20.1), in order to control different functions of the motor or other ancillary devices in the vehicle. In order to ensure a compact construction which is easy to use, the inventive device prevents the key (50) from turning in the slot (11) and the key (50) is displaced into at least three operating positions (20.1) for the control functions which are axially staggered. After being inserted for a first operating distance (51), the key takes up an initial position (20.1), in which it is secured in the slot (11) in a force-fit. In a subsequent second intermediate position, the key (50) is secured in a positive fit which can be locked automatically. This prevents the manual withdrawal (57) of the key (50). In order to remove the key (50), the latter is axially pushed into a third final position, in which the lock on the operating position can be released. During its course of operation, the key (50) is axially spring-tensioned (41) in the direction of the retaining position. The operating position of the key (50) determines the different vehicle functions.

(57) Zusammenfassung: Bei einer Vorrichtung zum Starten eines Motors wird eine Aufnahme (11) zum Einstecken (59) des Schlüssels (50) verwendet, die normalerweise von einer federnden Abdeckung (14) verschlossen ist. Der Schlüssel (50) wird in der Aufnahme (11) in verschiedene Schlüssellagen (20.1) überführt, um verschiedene Funktionen vom Motor oder weiteren Zusatzgeräten im Fahrzeug zu steuern. Um einen platzsparenden Aufbau und

[Fortsetzung auf der nächsten Seite]

WO 01/14179 A1

IPR2022-00412
Apple EX1053 Page 496

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht:
— *Mit internationalem Recherchenbericht.*
— *Mit geänderten Ansprüchen.*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

eine einfache Betätigung zu gewährleisten, wird vorgeschlagen, den Schlüssel (50) in der Aufnahme (11) unverdrehbar zu machen und für die Steuerung den Schlüssel (50) in mindestens drei zueinander axial versetzte Hublagen (20.1) zu überführen. Nach einer ersten Hubstrecke (51) des eingeführten Schlüssels kommt der Schlüssel in einer Anfangslage (20.1), wo er in der Aufnahme (11) kraftschlüssig festgehalten wird. Eine formschlüssige Sicherung des Schlüssels (50) ergibt sich in einer dann folgenden zweiten Mittellage, welche selbsttätig verriegelbar ist. Dann ist ein manuelles Herausziehen (57) des Schlüssels (50) verhindert. Zur Entnahme des Schlüssels (50) wird dieser in eine dritte Endlage axial eingedrückt, wo die Verriegelung der Betriebslage aufgehoben werden kann. Bei diesen Hubbewegungen ist der Schlüssel (50) in Richtung auf die Haltelage axial federbelastet (41). Die verschiedenen Funktionen des Fahrzeugs werden durch die Hublage des Schlüssels (50) mitbestimmt, (Fig. 5).

IPR2022-00412
Apple EX1053 Page 497

Vorrichtung zum Starten eines Fahrzeugmotors mittels eines elektronischen Schlüssels

Die Erfindung richtet sich auf eine Vorrichtung der im Oberbegriff des Anspruches 1 angegebenen Art. Solche Vorrichtungen werden üblicherweise als elektronisches „Zündschloss" bzw. „Zünd-Lenk-Schloss" bezeichnet. Mit einem elektronischen Schlüssel wird üblicherweise der Zugang zum Fahrzeug gesichert und entsichert. Dafür sind geeignete Türschlösser vorgesehen. Bei der Verwendung dieses Schlüssel bei der hier interessierenden Vorrichtung wird der Schlüssel in eine im Kraftfahrzeug vorgesehene Aufnahme eingesteckt. In manchen Fällen wird dabei eine dort vorgesehene Abdeckung weggedrückt. Zur Steuerung von verschiedenen Funktionen im Kraftfahrzeug wird der eingesteckte Schlüssel in der Aufnahme in verschiedene Schlüssellagen überführt.

Bei der bekannten Vorrichtung dieser Art (DE 44 34 655 A1) werden die verschiedenen Funktionen durch entsprechende Drehstellungen des elektronischen Schlüssels in der Aufnahme angewählt. Dazu besteht die Aufnahme aus einem Rotor und einem Stator und verschiedenen Sensoren am Stator, welche die verschiedenen Drehstellungen des Rotors zu ermitteln haben. Das ist bau- und platzaufwendig. Um das erforderliche Drehmoment zur Verstellung des Schlüssels manuell ausüben zu können, muss der Schlüssel ausreichend weit aus der Öffnung der Aufnahme herausragen. Ein weit herausragender Schlüssel erhöht aber beim Crashfall des

IPR2022-00412
Apple EX1053 Page 498

Fahrzeugs die Verletzungsgefahr. Zusätzlich oder alternativ zur rotatorischen Bewegung kann auch eine translatorische Bewegung des Schlüssels stattfinden.

Bei einer Vorrichtung anderer Art (DE 198 14 964 A1) wird das Fahrberechtigungssignal durch eine Detektion eines Fingerabdrucks der berechtigten Person erzeugt. Dabei wird ein Autorisierungselement in Form einer Scheckkarte verwendet, welche in einen Schlitz neben einem Wippschalter oder in einem Drehschalter eingeführt wird. Der Drehschalter und der Wippschalter besitzen Sensoren für den Fingerabdruck und sind zwischen verschiedenen Schalterlagen druckbetätigbar oder verdrehbar. Dadurch werden verschiedene Funktionen des Motors gesteuert. In diesem Fall sind außer der Einsteckbewegung des Autorisierungselements sowohl eine Drehung oder Druckbewegung eines Schalters als auch die Anbringung eines Fingerabdrucks an der den Sensor aufweisenden Stelle erforderlich. Diese komplexe Betätigung ist umständlich.

Schließlich ist es bekannt, bei einem Startschalter für ein Kraftfahrzeug (DE 195 04 991 C1) in einem Drehgriff einen Schacht zur vollständigen Einführung einer Identifikationskarte vorzusehen. Diese Einführung ist nur in einer ersten Position des Drehgriffs möglich. Von dieser Position ausgehend kann dann der Drehgriff mit der eingesteckten Karte in verschiedene weitere Drehpositionen überführt werden, welche verschiedene Funktionen des Motors steuert. In diesem Fall sind außer den Steckbewegungen auch noch rotative Bewegungen des Drehgriffs erforderlich.

Der Erfindung liegt die Aufgabe zugrunde, eine zuverlässige, bequem betätigbare Vorrichtung der im Oberbegriff des Anspruches 1 genannten Art zu entwickeln, welche die vorerwähnten Nachteile vermeidet. Dies wird erfindungsgemäß durch die im Kennzeichen des Anspruches 1 angeführten Maßnahmen erreicht, denen folgende besondere Bedeutung zukommt.

Bei der Erfindung wird der Schlüssel zur Funktionsauswahl nicht gedreht. Der Schlüssel wird vielmehr beim Einschieben in die Aufnahme in drei zueinander axial versetzte Hublagen überführt, von denen aber für die Zündung des Motors die zweite Hublage maßgeblich ist. In dieser zweiten Hublage ist der Schlüssel nahezu ganz in

der Aufnahme eingeführt. In dieser zweiten Hublage und in der noch tieferen dritten Hublage werden die wesentlichsten Funktionen im Kraftfahrzeug ausgeführt, wofür fallweise weitere manuelle Betätiger oder Pedale genutzt werden. Der Kraftfahrzeugbenutzer braucht nicht am Schlüssel Betätigungen auszuführen, um die gewünschten Funktionen im Fahrzeug auszulösen. Der Schlüssel bleibt vielmehr in der Aufnahme weitgehend versenkt, weshalb im Crashfall keine Verletzungsgefahr durch weit herausragende Schlüsselteile zu befürchten ist.

In seiner zweiten Hublage ist der Schlüssel durch ein Richtgesperre in der Aufnahme fixiert, dessen formschlüssige Haltemittel den Schlüssel gegenüber einer axialen Federkraft sichern. Um den Schlüssel wieder entnehmen zu können, genügt es ihn an seinem Ende anzutippen. Dann wird der Schlüssel in seine dritte Hublage überführt. Das Schlüsselende kann sich dabei beliebig tief in der Aufnahme befinden. In dieser dritten Hublage kann die Verriegelung fallweise freigegeben werden. Dann wird der Schlüssel aufgrund einer auf ihn mittelbar oder unmittelbar einwirkenden axialen Rückstellfederung wieder in seine Anfangslage zurückgedrückt. Dann liegt nur eine kraftschlüssige Verbindung eines Rastgesperres vor. Der Schlüssel kann manuell wieder entnommen werden. Bei der Erfindung sind folglich nur axiale Bewegungen des elektronischen Schlüssels zwischen mindestens drei Hublagen erforderlich, um den Motor oder weitere Zusatzgeräte im Kraftfahrzeug zu steuern. Diese axiale Bewegung ist mit dem Einstecken des Schlüssels in die Aufnahme des Fahrzeugs gleichgerichtet. Es liegt also eine sehr sinnfällige Handhabung des Schlüssels bei der erfindungsgemäßen Vorrichtung vor.

Weitere Maßnahmen und Vorteile der Erfindung ergeben sich aus den Unteransprüchen, der nachfolgenden Beschreibung und den Zeichnungen. In den Zeichnungen ist die Erfindung schematisch in zwei Ausführungsbeispielen dargestellt, von denen jedes der beiden von eigenständiger erfinderischer Bedeutung ist. Das erste Ausführungsbeispiel ist in den Fig. 1 bis 8 und das zweite Ausführungsbeispiel in den Fig. 9 bis 14 veranschaulicht. Es zeigen:

Fig. 1, einen Axialschnitt durch die Vorrichtung des ersten Ausführungsbeispiels, längs der Schnittlinie I - I von Fig. 3, wobei die Bauteile sich in einer Ausgangsstellung vor dem Einstecken eines zugehörigen elektronischen Schlüssels befinden,

Fig. 2 die in Fig. 1 gezeigte Vorrichtung in einem demgegenüber rechtwinklig versetzten Axialschnitt, der in Fig. 3 mit II - II gekennzeichnet ist, bei gleicher Stellung der Bauteile,

Fig. 3 einen Querschnitt durch die Vorrichtung, längs der in Fig. 1 mit III - III gekennzeichneten Schnittlinie,

Fig. 4 die stirnseitige Draufsicht auf die Vorrichtung von Fig. 1 bis 3,

Fig. 5, in einer der Fig. 1 entsprechenden Darstellung eine erste Hublage der Bauteile, die sich nach einem anfänglichen Einstecken des elektronischen Schlüssels ergibt,

Fig. 6 eine durch weiteres axiales Einstecken des Schlüssels in die Aufnahme von Fig. 5 sich ergebende zweite Hublage der Bauteile der in Fig. 1 gezeigten Vorrichtung,

Fig. 7 eine gegenüber Fig. 6 noch ein wenig tiefer liegende Hublage des eingesteckten Schlüssels, um ihn aus der zweiten Hublage von Fig. 6 in die in Fig. 5 erläuterte erste Hublage zu überführen,

Fig. 8 die Vorderansicht auf eine im Gehäuse der Vorrichtung vorgesehene Leiterplatte, teilweise im Einbauzustand im Gehäuse,

Fig. 9 in Analogie zu Fig. 6, einen entsprechenden Axialschnitt durch das zweite Ausführungsbeispiel der erfindungsgemäßen

IPR2022-00412
Apple EX1053 Page 501

Vorrichtung, wenn sich der Schlüssel in seiner zweiten Hublage befindet,

Fig. 10 die in Fig. 9 gezeigte zweite Vorrichtung nach der Erfindung bei gleicher Stellung der Bauteile, allerdings in einem gegenüber Fig. 9 rechtwinklig versetzten Axialschnitt durch die Vorrichtung,

Fig. 11 nur einige Bauteile der in Fig. 9 gezeigten Vorrichtung in einer Ausgangsstellung, die sich bei einem aus der Vorrichtung entnommenen Schlüssel ergibt und

Fig. 12-14, in einer der Fig. 11 entsprechenden Darstellung, die Stellung der Bauteile, wenn sich der Schlüssel in drei verschiedenen Hublagen befindet, in Analogie zu den in Fig. 5, 6 und 7 gezeigten Schlüssellagen des ersten Ausführungsbeispiels.

Das in Fig. 1 bis 8 gezeigte erste Ausführungsbeispiel der erfindungsgemäßen Vorrichtung besitzt eine Aufnahme 11 zum Halten eines elektronischen Schlüssels. Die Aufnahme 11 befindet sich im Inneren eines Gehäuses 10. Dieses Gehäuse 10 kann in einer Armatur im Fahrzeuginneren integriert sein, deren Kontur 12 strichpunktiert in Fig. 1 und 2 angedeutet ist. Die Fig. 1 bis 4 zeigen die Vorrichtung bei entnommenen Schlüssel 50. Dann ist die stirnseitige Öffnung 13 der Aufnahme 11 durch eine Abdeckung 14 verschlossen.

Die Abdeckung 14 ist relativ zu einem im Gehäuse 10 vorgesehenen Schieber 20 mit einer leichten Druckfeder 15 belastet und dort zwischen zwei Stellungen, nämlich 14.1 von Fig. 1 und 14.2 axial von Fig. 5 verschieblich. Diese beiden Stellungen 14.1 und 14.2 sind durch einen vorderen und einen hinteren Endanschlag 22, 29 im Schieber 20 bestimmt. Bei entnommenen Schlüssel gemäß Fig. 1 bis 4 liegt die vordere Ausschubstellung 14.1 der Abdeckung 14 vor, wo die Öffnung 13 verschlossen ist. Dann kann Schmutz in das Innere der Aufnahme 11 nicht eindringen. Die Abdeckung 14 befindet sich dann, unter Wirkung ihrer Druckfeder

IPR2022-00412
Apple EX1053 Page 502

15 am vorderen Endanschlag 22. Die andere Stellung 14.2 gemäß Fig. 5 wird auf folgende Weise erreicht.

Damit der Schlüssel 50 mit der Vorrichtung zusammenwirken kann, ist eine durch den Pfeil 59 in Fig. 1 und 2 verdeutlichte Einsteckbewegung des Schlüssels 50 in die Aufnahme 11 erforderlich. Dabei kommt der Schlüssel mit der Abdeckung 14 in Berührung. Das ist die strichpunktiert in Fig. 1 und 2 verdeutlichte axiale Lage 50.0. Dabei taucht der Schlüssel mit einem Vorderstück 58 in eine entsprechende Aussparung der Abdeckung 14 bereits ein, welche zu der nachfolgenden Aufnahme 11 im Gehäuse 10 noch hinzukommt. Diese Lage 50.0 des Schlüssels 50 soll nachfolgend kurz „Berührungslage" bezeichnet werden. Davon ausgehend sollen alle weiteren Hublagen des Schlüssels anhand von Fig. 5 bis 7 beschrieben werden.

Nach einer anfänglichen Einsteckbewegung 59 um eine aus Fig. 5 ersichtliche erste Hubstrecke 51 kommt der Schlüssel in seine in Fig. 5 mit 50.1 gekennzeichnete erste axiale Hublage. Dabei wird, wie bereits erwähnt wurde, die Abdeckung 14 zurückgedrückt und kommt an ihrem zweiten Endanschlag 29 im Inneren des Schiebers 20 zur Anlage. Die Öffnung 13 der Aufnahme ist zwar frei, aber jetzt durch den eingesteckten Schlüssel 50 verschlossen. Die Abdeckung 14 befindet sich dann in ihrer Einschubstellung 14.2. In dieser Hublage 50.1 wird der Schlüssel 50 kraftschlüssig in seiner Aufnahme 11 gehalten wofür die Halteelemente 21, 22, 55 sorgen, deren Aufbau am besten anhand von Fig. 1 zu erkennen ist. Der Schieber 20 ist dosenförmig ausgebildet, wobei die Dosenwand stellenweise eine radial federnde Zunge 21 aufweist, welche ein erstes Halteelement bildet. Diese Zunge 21 ist zunächst ein erster Bestandteil eines zwischen Schlüssel 50 und Schieber 20 bestehenden Rastgesperres. Am Ende der Zunge 21 befindet sich nämlich ein radialer Vorsprung 22, der ein weiteres Halteelement des Rastgesperres darstellt. Dieser Vorsprung 22 kann im Übrigen auch die bereits erwähnten Anschlagfunktionen in der Ausschubstellung 14.1 der Abdeckung 14 erfüllen. Beim Einstecken 59 des Schlüssels 50 führen die Zungen 21 kurzzeitig eine radiale Spreizbewegung aus, bis der an den Zungen 21 sitzende Vorsprung 22 in eine zugeordnete Rastvertiefung 55 am Schlüssel kraftschlüssig eingreift. Das ist in Fig. 5 gegeben. Die Rastvertiefung 55 ist ebenfalls Bestandteil des erwähnten Rastgesperres. Diese erste Hublage 50.1

IPR2022-00412
Apple EX1053 Page 503

soll nachfolgend kurz „Anfangslage" des Schlüssels bezeichnet werden. In dieser Anfangslage 50.1 liegt eine kraftschlüssige Sicherung des Schlüssels in der Aufnahme 11 vor.

Die vorerwähnte Spreizbewegung der Zunge 21 beim Einstecken 59 des Schlüssels ist möglich, obwohl die Zunge 21 auf ihrer dem rastwirksamen Vorsprung 22 gegenüberliegenden Seite einen radialen Gegenvorsprung 23 aufweist. In diesem Bereich besitzt nämlich das Gehäuse 10 eine aus Fig. 1 erkennbare radiale Aussparung 16, in welche dieser Gegenvorsprung 23 beim Schlüsseleinstecken 29 radial ausweichen kann.

Ausweislich der Draufsicht von Fig. 4 ist die Öffnung 13 für die Aufnahme durch eine Blende 17 umgrenzt, die Führungsmittel 18 für den Schlüssel 50 besitzt. Diese bestehen hier aus zwei einander gegenüberliegend angeordneten Stegen 18 an der Blende 17. Die zugehörigen Führungsmittel 54 am Schlüssel bestehen, wie aus Fig. 1 und 2 hervorgeht, aus einer Längsnut. Diese beiseitigen Längsnuten 54 sorgen für ein gutes axiales Einstecken 59 des Schlüssels 50, auch wenn die Außenflächen des Schlüssels aus stilistischen Gründen nicht achsparallel ausgeführt sein sollten. Die vorerwähnte haltewirksame Rastvertiefung 55 ist im Übrigen im Bereich dieser Längsnut 54 angeordnet. Der in seine Anfangslage 50.1 von Fig. 5 befindliche Schlüssel 50 kann von Hand wieder im Sinne des Pfeils 57 von Fig. 5 manuell herausgezogen werden. Dann fährt die Abdeckung 14 wieder in ihre Ausschubstellung 40.1 von Fig. 1 zurück. Der Schlüssel kann auch in einer um 180 ° gewendeten Position eingesteckt werden.

Das Herausziehen 57 des Schlüssels ist aber verhindert, wenn der Schlüssel, ausgehend von seiner Anfangslage 50.1 von Fig. 5 um eine weitere, beträchtliche Hubstrecke 52 bis zu seiner in Fig. 6 erkennbaren zweiten axialen Hublage 50.2 überführt worden ist. Dann ist nämlich der Schlüssel 50 sogar formschlüssig in der Aufnahme 11 gesichert. An diesem Formschluss sind zunächst die gleichen Halteelemente 21, 22, 55 wie beim Rastgesperre beteiligt, das vorausgehend für den kraftschlüssigen Zusammenhalt zwischen dem Schieber 20 und dem Schlüssel 50 sorgte. Der an der federnden Zunge 21 vom Schieber 20 vorgesehene

IPR2022-00412
Apple EX1053 Page 504

Gegenvorsprung 23 kommt in diese Hublage 50.2 an einer aus Fig. 6 erkennbaren radialen Stützfläche 19 im Gehäuse 10 zu liegen. Diese Stützfläche 19 befindet sich unterhalb der vorausgehend in der Anfangslage 50.1 damit ausgerichteten radialen Aussparung 16. In seiner Hublage 50.2 wird also der Schlüssel 50 in der Aufnahme 14 formschlüssig verriegelt. Ein Herausziehen 57 im Sinne des auch in Fig. 6 eingezeichneten Pfeils ist nicht möglich. Diese zweite Hublage 50.2 des Schlüssels soll nachfolgend kurz „Mittellage" bezeichnet werden.

Die axiale Position des Schiebers 20 von Fig. 5 oder 6 wird durch eine weitere Einsteckbewegungen 59 des Schlüssels 50 erreicht. In Fig. 5 befindet sich der Schieber 20 in einer dort mit 20.1 gekennzeichneten Ausgangsposition, welche die äußere Position des Schiebers im Gehäuse 10 ist. Diese Ausgangsposition 20.1 liegt im Übrigen auch in Fig. 1 bzw. Fig. 2 vor, wo der Schlüssel 50 ganz entfernt ist oder mit der Abdeckung 14 in Berührung 50.0 kommt. Die vorgenommene Hublage 50.2 des Schlüssels 50 ist zunächst gesichert, weil der den Schlüssel 50 aufnehmende Schieber 20 in der zugehörigen Axialposition 20.2 verriegelt wird. Dafür dient ein hier als federnde Klinke 30 ausgebildeter Riegel, der einen Sperrarm 31 und einen damit drehfesten Stellarm 32 aufweist. Der Riegel 30 ist bei 33 ortsfest im Gehäuse 10 schwenkbar gelagert und greift mit seinem Sperrarm 31 in den Betätigungsweg einer Schulter 24, die beim Axialbewegen des Schiebers 20 mitbewegt wird. Die Schulter 24 befindet sich hier an einem Nocken, der Bestandteil eines aus Fig. 5 erkennbaren Axialansatzes 25 des Schiebers 20 ist. Der Axialansatz 25 taucht beim Bewegen des Schiebers 20 entlang der Hubstrecke 52 teleskopartig in eine gehäusefeste Hülse 45 ein.

Die Gehäusehülse 45 und der Axialansatz 25 dienen im Übrigen auch zur Aufnahme einer kräftigen Rückstellfeder 40, die bestrebt ist, den Schieber 20 in dessen Ausgangsposition 20.1 zu halten. Dazu ist zweckmäßigerweise auch der Axialansatz 25 vom Schieber 20 rohrförmig ausgebildet und besitzt einen Innenbund 26 an dem sich das obere Ende der Rückstellfeder 40 abstützt. Der obere Bereich dieses rohrförmigen Axialansatzes 25 kann seinerseits als Aufnahme für die bereits oben beschriebene Abdeck-Druckfeder 15 dienen, die demgegenüber sehr viel weicher ausgebildet ist. Die Rückstellfeder 40 übt auf den Schieber 20 eine durch den Pfeil

41 in Fig. 5 verdeutlichte Rückstellkraft aus. Dadurch wird der Schieber 20 gegen einen gehäusefesten Endanschlag 42 gedrückt, der hier durch die Innenfläche der beschriebenen Blende 17 gebildet wird. Dieser Anschlag 42 bestimmt die Ausgangsposition 20.1 des Schiebers 20. Der Nocken mit der Schulter 24 befindet sich in der Ausgangsposition 20.1 des Schiebers 20 noch axial oberhalb der Klinke 30.

Die Schulter 24 wirkt mit der Klinke 30 nach Art eines sogenannten „Richtgesperres" zusammen. Der Sperrarm 31 befindet sich mit seinem Sperrende in dem durch eine Punktlinie 27 in Fig. 5 veranschaulichten Verschiebungsweg 27 der Schulter 24. Bei der Einsteckbewegung 59 von Fig. 5 fährt der die Schulter 24 tragende Nocken gegen den Sperrarm 31 der Klinke 30 und drückt diese weg, bis die Schulter 24 in ihrer aus Fig. 6 ersichtliche Position gekommen ist. Dann schnappt der Sperrarm 31 vor die Schulter 24 und hält den Schieber 20, gegen die axiale Federbelastung 41 in der Axialposition 20.2 fest. Eine Rückbewegung des Schiebers 20 in die vorausgehende Axialposition 20.1 ist zunächst nicht möglich.

Die der Mittellage 50.2 des Schlüssels 50 von Fig. 6 entsprechende Axialposition 20.2 des Schiebers 20 soll als „Arbeitsposition" bezeichnet werden. In dieser Mittellage 50.2 erkennt zunächst eine elektronische Steuereinheit der Vorrichtung z.B. auf elektrischem oder elektromagnetischem Weg, dass es sich um den richtigen Schlüssel 50 handelt. Als Identifikationsmittel dient im vorliegenden Fall ein im Gehäuse 10 integrierter Transponder 43, der Bestandteil der nicht näher gezeigten elektrischen Steuereinheit ist. Wenn die Übereinstimmung des Schlüssels 50 mit der Vorrichtung festgestellt ist, schaltet die Steuereinheit ihre elektrischen Ausgänge und/oder Eingänge wirksam. Eine bis dahin bestehende eventuelle Sperre der Fahrzeuglenkung wird entriegelt. Vor allem werden Sensoren 44 wirksam gesetzt, die zu einem hier manuell bedienbaren Betätiger 35 gehören. Mit diesen Sensoren 44 werden die gewünschten verschiedenen Funktionen im Fahrzeug ausgewählt.

Der Betätiger 35 besteht im vorliegenden Fall aus einem Taster, der, wie am besten aus Fig. 2 und 8 zu erkennen ist, in einem Nachbarbereich des gleichen Gehäuses 10 integriert sein kann. Der Taster 35 ist aufgrund einer Axialführung 34 im Sinne des

Druckpfeils 36 von Fig. 8 axial betätigbar und wird mittels einer Rückstellfeder 37 und entsprechende Endanschläge in seine Ausgangsstellung von Fig. 2 zurückgeführt. Welche Betätigungen zu welchen Funktionen im Fahrzeug führen, hängt von der Programmierung der elektrischen Steuereinheit ab. Eine Möglichkeit besteht darin, dass beim ersten Drücken 38 des Tasters 35 ein Radio sowie eine Elektronik im Fahrzeug eingeschaltet wird, z.B. das Parklicht, der Antrieb für Fensterheber, die motorische Sitzverstellung und das Schiebedach. An der Funktionssteuerung der Elektronik können auch noch andere, an sich übliche Steuerglieder im Fahrzeug beteiligt sein, z.B. die Fußbremse. Die vorerwähnte Radioeinstellung erfolgt in diesem Fall ohne Betätigung der Fußbremse. Die weiteren Funktionen im Fahrzeug können auf folgende Weise ausgelöst werden.

Durch ein zweites Drücken 36 des Tasters 35, ohne gleichzeitige Betätigung der Fußbremse, erfolgt beispielsweise die Zündung des Motors. Wird der Taster 35 gedrückt 36 und gleichzeitig die Fußbremse getreten, dann startet der Motor. Wird daraufhin der Taster 35 nochmals gedrückt 36, so geht der Motor wieder aus. Letzteres kann dann mit oder ohne Betätigung der Fußbremse erfolgen.

Diese Funktionen können auch optisch im Bereich des Tasters 35 angezeigt werden, wie am besten anhand von Fig. 8 zu entnehmen ist. Über die Steuerelektronik wird bei der Funktion „Start" eine erste Diode 46 angesteuert, die ein Teil-Schriftfeld 38 des Tasters 35 gemäß Fig. 4 beleuchtet. Lichttrennwände 39 sorgen für eine entsprechende Teilbelichtung auf der Schauseite des Tasters 35. Bei der Funktion „Stop" wird durch die Steuereinheit dagegen eine zweite Diode 46' bestromt, worauf dann im Nachbar-Schriftfeld 38' die Beleuchtung eingeschaltet wird und die schauseitige Beschriftung im Taster 35 ablesbar macht.

Die Verriegelung des Schlüssels 50 in der Mittellage 50.2 erfolgt, wie oben beschrieben wurde, durch den Sperrarm 31 der Klinke 30, der über die Schulter 24 auch den Schieber 20 in dessen entsprechende Arbeitsposition 20.2 festhält. Die Klinke 30 befindet sich aufgrund ihrer nicht näher gezeigten Drehfederbelastung und entsprechender Drehanschläge normalerweise in ihrer Sperrposition von Fig. 6. Der Schlüssel 50 ist dabei größtenteils in der Aufnahme 11 versenkt angeordnet und ragt

IPR2022-00412
Apple EX1053 Page 507

nur mit einem minimalen Endstück 56 aus der Aufnahme 11 gemäß Fig. 6 heraus. Um den Schlüssel 50 aus der Mittellage 50.2 lösen zu können, muss der Schlüssel 50 zunächst in eine noch tiefere Hublage 50.3 gemäß Fig. 7 im Sinne des dortigen Einsteckpfeils 59 eingedrückt werden. Diese Hublage 50.3 kurz „Endlage" bezeichnet werden. In Fig. 7 sind die vorausgehenden Hublagen 50.0 bis 50.2 ebenfalls strichpunktiert eingezeichnet.

Zum Übergang von Fig. 6 auf Fig. 7 wird der Schlüssel 50 nur noch um eine verhältnismäßig kleine dritte Hubstrecke 53 gemäß Fig. 7 gegen die axiale Federkraft 41 eingedrückt. Der Schlüssel erreicht dann seine unterste dritte Hublage 50.3, welche natürlich wieder einer entsprechenden Endposition 20.3 des Schiebers 20 entspricht. Diese Endposition 20.3 wird von weiteren Sensoren 47 erfasst, die zu der erfindungsgemäßen Steuereinheit gehören. Im Ansprechfall schaltet die Steuereinheit einen Antrieb 48 ein, der hier aus einem elektrischen Hubmagneten besteht. Dieser Hubmagnet 48 bewegt einen Stößel 49 od. dgl. in eine Arbeitsposition, in welcher er den vorerwähnten Stellarm 32 der Klinke 30 trifft. Weil der Stellarm 32 drehfest mit dem Sperrarm 31 ist, wird durch diese Schwenkbewegung gemäß Fig. 7 der Sperrarm 31 aus seiner bisherigen Sperrposition wegbewegt. Die Schulter 24 wird freigegeben. Die Blockade des Schiebers 20 ist dann aufgehoben. Der Schieber 20 wird aufgrund der wirkenden Federkraft 41 im Sinne des Bewegungspfeils 57 von Fig. 7 automatisch zurückbewegt. Der Sperrarm 31 bleibt dabei solange durch den Hubmagneten 48 in seiner entriegelten Position von Fig. 7, bis die mit dem Schieber 20 mitbewegliche Schulter 24 sich an seinem Sperrende vorbeibewegt hat; d.h. bis kurz nach der aus Fig. 6 erkennbaren Mittellage 50.2 des Schlüssels.

Nach der Entriegelung von Fig. 7 bewegt die axiale Federkraft 41 den Schieber 20, und mit ihm den Schlüssel 50 bis sich wieder die Verhältnisse von Fig. 5 ergeben. Der Schieber 20 stoppt erst in seiner dortigen Ausgangsposition 20.1, wo die Federkraft 41 von dem erwähnten Endanschlag 42 für den Schieber 20 aufgenommen wird. Der Schlüssel 50 steckt aber immer noch in seiner Aufnahme 11. Jetzt ragt der Schlüssel 50 allerdings mit einem größeren Teilstück 28 aus der Aufnahme 11 heraus. Er kann mit der Hand bequem erfasst und manuell ganz im Sinne des Pfeils

IPR2022-00412
Apple EX1053 Page 508

57 herausgezogen werden. In der Anfangslage 50.1 von Fig. 5 liegt nämlich wieder die beschriebene kraftschlüssige Halterung des Schlüssels 50 im Schieber 20 vor.

Durch eine plötzliche Rückstellbewegung des Schiebers 20 aus der Endposition von Fig. 2.3 in die Ausgangsposition 20.1 von Fig. 5 könnte der Schlüssel 50 Beschleunigungskräften ausgesetzt sein, die ihn aus der Aufnahme 11 heraus katapultieren, über seine kraftschlüssige Anfangslage 50.1 in Fig. 5 hinaus. Dies lässt sich leicht durch eine geeignete Dämpfungseinrichtung 60 beheben. Diese besteht im vorliegenden Fall aus einem Dämpfungsrad 60, das ortsfest im Gehäuse 10 bei 61 drehgelagert ist, wie aus Fig. 1 und 2 zu erkennen ist. Das Dämpfungsrad 60 steht über ein Stirnrad 62 in Zahneingriff mit einer Zahnstange 63, die mit dem Schieber 20 mitbeweglich ist. Die Zahnstange 63 kann in den vorerwähnten Axialansatz 25 gemäß Fig. 1 und 2 integriert sein, wo auch der Nocken für die Schulter 24 sitzt. Sofern als Sensor 47 ein Mikroschalter verwendet wird, kann der entsprechende Schaltnocken 64 an diesem Ansatz 25 sitzen.

Die erwähnte Steuereinheit ist über die am unteren Gehäuseende vorgesehenen Steckkontakte 65 mit den elektrischen Bauteilen im Inneren des Gehäuses 10 verbunden. Man kann dazu eine auch aus Fig. 8 erkennbare Leiterplatte 66 nutzen, die durch geeignete Zwischenböden 67 in ihrer Position im Inneren des Gehäuses gemäß Fig. 3 gehalten wird.

Wie erwähnt wurde, wird der Schlüssel 50 aus seinem Formschluss in Fig. 6 über Fig. 7 auf elektromechanische Weise freigegeben und selbsttätig in seine Anfangslage 50.1 von Fig. 5 zurückgeführt. Die Bedingung hierfür, welche die erwähnte elektrische Steuereinheit überwacht, ist, dass der Motor des Fahrzeugs ausgeschaltet ist. Wenn man, bei eingeschaltetem Motor, in der Mittellage 50.2 den Schlüssel 50 eindrückt, so wird der beschriebene Hubmagnet 48 nicht wirksam gesetzt; die Klinke 30 bleibt sperrwirksam und fängt den Schlüssel wieder in der Mittellage 50.2 von Fig. 6. Damit ist eine Fehlbedienung der erfindungsgemäßen Vorrichtung ausgeschlossen.

Eine Alternative kann aber darin bestehen, dass bei stehendem Fahrzeug, wo die Räder sich nicht mehr drehen, der Motor noch an ist. Auch dies wird von der elektrischen Steuereinheit registriert. Wird dann wieder im Sinne von Fig. 7 auf den Schlüssel 50 gedrückt, so kann über einen Impulsschalter der Motor ausgeschaltet werden. Der beschriebene Formschluss des Schlüssels 50 wird dann wieder elektromechanisch freigegeben und kann über die Kraftschlussraste aus einer Anfangslage 50.1 in Fig. 5 manuell entnommen werden.

Wie bereits erwähnt wurde, zeigen die Fig. 9 bis 14 den Aufbau und die Wirkungsweise eines zweiten Ausführungsbeispiels der erfindungsgemäßen Vorrichtung, welcher eine eigenständige erfinderische Bedeutung zukommt. Zur Benennung analoger Bauteile sind die gleichen Bezugszeichen wie im ersten Ausführungsbeispiel verwendet, weshalb insoweit die bisherige Beschreibung gilt. Es genügt lediglich auf die Unterschiede einzugehen. Bei dieser Vorrichtung besitzt der Schlüssel 50 die Form einer Scheckkarte.

Die stirnseitige Öffnung 13 der dortigen Aufnahme 11 besteht aus einem Schlitz im Gehäuse 10. Die Abdeckung 14' der Öffnung 13 erfolgt hier durch eine Klappe, deren Aufklapplage in Fig. 10 ausgezogen und deren Zuklapplage bei entnommenem Schlüssel in Fig. 10 strichpunktiert angedeutet ist. Identifikationsmittel für den Schlüssel 50 sind im Gehäuse 10 integriert und bestehen auch in diesem Fall z.B. aus einem Transponder 43. Einen Schieber 20, wie im ersten Ausführungsbeispiel, gibt es nicht. Die Haltemittel und Verriegelungen wirken unmittelbar mit dem Schlüssel 50 zusammen, dessen am besten aus Fig. 11 erkennbarer Scheckkartenumriss 68 in geeigneter Weise profiliert ist. Auch in diesem Fall kann der Schlüssel 50 in der Aufnahme 11 in drei axiale Hublagen 50.1, 50.2 und 50.3 überführt und positioniert werden. Diese drei Hublagen sind in Fig. 9 durch Höhenlinien veranschaulicht und in Fig. 12 bis 14 zusammen mit den damit zusammenwirkenden Bauteile verdeutlicht.

Beim Einschieben 59 des Schlüssels 50 wird zunächst die in Fig. 12 gezeigte Anfangslage 50.1 des Schlüssels 50 erreicht, wo der Schlüssel 50 durch ein Rastgesperre 70 kraftschlüssig im Gehäuse 10 gesichert ist. Auch in diesem Fall besteht das Halteelement 71 aus einer radial federnden Zunge, doch ist diese, im

IPR2022-00412
Apple EX1053 Page 510

Gegensatz zum ersten Ausführungsbeispiel, ortsfest im Gehäuseinneren positioniert. Zum Rastgesperre 70 gehört eine Rastvertiefung 55 im Schlüssel 50, die durch ein entsprechendes Kantenprofil seines erwähnten Kantenumrisses 68 erzeugt ist. Ein radialer Vorsprung 75 an der Zunge 71 untergreift kraftschlüssig eine Haltekante 76 an der Rastvertiefung 55.

Weil es in diesem Fall, wie gesagt, einen Schieber nicht gibt, wirken in Fig. 9 angedeutete Rückstellkräfte 41 unmittelbar auf den Schlüssel 50 ein. Maßgeblich dafür sind hier doppelt vorgesehene Rückstellfedern 40, 40', die über einen zugehörigen Stößel 74 bzw. 74', welcher auf die Unterkante 69 des Schlüsselumrisses 68 drücken können. In Fig. 12 ist gerade der eine Stößel 74 in Kantenberührung und übt eine nur geringe Rückstellkraft 41 aus. Die kraftschlüssige Haltekraft der federnden Zunge 41 reicht jedenfalls aus, um die Anfangslage 50.1 des Schlüssels 50 von Fig. 12 sicherzustellen. Eine Entnahme 57 des Schlüssels ist gegen die Wirkung des Rastgesperres 70 in Fig. 12 möglich.

Auch bei diesem zweiten Ausführungsbeispiel lässt sich der Schlüssel 50 von der Anfangslage 50.1 um eine Hubstrecke 52 in die aus Fig. 13 ersichtliche zweite Mittellage 50.2 in der Aufnahme 11 der Vorrichtung weiterschieben 59. Auch in diesem Fall kommt es in der Mittellage 50.2 zu einem Formschluss. Die hierfür maßgeblichen Halteelemente 81 sind in diesem Fall, im Gegensatz zum ersten Ausführungsbeispiel, nicht Bestandteil des Rastgesperres 70, sondern gehören zu einem davon gesonderten Gesperre 80, welches eine mehrfache Funktion zu erfüllen hat. Dieses Gesperre besteht im vorliegenden Fall aus einer Klinke 80, die an einem ortsfesten Lager 84 im Gehäuse 10 schwenkgelagert ist. Eine Klinken-Federbelastung 85 ist bestrebt die Klinke 80 in ihrer aus Fig. 11 ersichtlichen Lage zu halten, wo sie mit einem Stellarm 82 auf den Betätiger 73 eines hier als Mikroschalter ausgebildeten Sensors 72 einwirkt. Dies liegt bereits bei entnommenen Schlüssel gemäß Fig. 11 vor. Dieser Stellarm 82 ist drehfest mit dem vorbeschriebenen Halteelement 81 dieses Verriegelungsgesperres 80 verbunden.

In der in Fig. 12 beschriebenen Ausgangslage 50.1 des eingesteckten Schlüssels 50 kommt das Halteelement 81 der Klinke 80 mit dem Profilbereich 79 der

IPR2022-00412
Apple EX1053 Page 511

Umrisskontur 68 in Berührung, durch welche die Klinke 80 gegen ihre Rückschwenkkraft 86 zurückgeschwenkt wird. Dadurch wird der Betätiger 73 des Klinken-Sensors 72 vom Stellarm 82 freigegeben. Das wird von einer auch bei dieser Vorrichtung vorgesehenen elektrischen Steuereinheit festgestellt, an die dieser Klinken-Sensor 72 angeschlossen ist. Der vorerwähnte Transponder 43 wird wirksam gesetzt und stellt fest, ob der „richtige Schlüssel" eingestellt ist. Nur beim richtigen Schlüssel werden bereits erste Funktionen im Fahrzeug von der Steuereinheit eingeschaltet, z.B. die Spannungsversorgung für ein Radio, für das Parklicht, für einen Antrieb eines Fensterhebers, einer motorischen Sitzverstellung und eines Schiebedachs.

Beim Weiterdrücken 52 des Schlüssels 50 in die bereits erwähnte Mittellage 50.2 von Fig. 13 kommt der Formschluss dadurch zustande, dass das Halteelement 81 ein Hakenende 87 aufweist, welches eine Schulter 88 vom Schlüssel 50 hintergreift. Jetzt ist eine Entnahme des Schlüssels im Sinne des Pfeils 57 blockiert. Bei der Verschiebung 52 des Schlüssels 50 von Fig. 12 auf Fig. 13 ist auch eine Hubarbeit gegen die von der Rückstellfeder 40 bedingte Rückstellkraft 41 ausgeübt worden. In Fig. 13 kommt aber auch die andere Rückstellfeder 40' mit ihrem Stößel 74' an der Unterkante 69 des Schlüsselprofils 68 zur Anlage. Die Schulter 88 gehört zu einem Randausbruch 89 im Scheckkartenumriss 68. Aufgrund seiner Rückschwenkkraft 86 ist daher die Klinke 80 wieder in ihrer bereits in Fig. 11 beschriebenen Ausgangs-Schwenkstellung, wo ihr Stellarm 82 den Betätiger 73 des Klinken-Sensors 72 drückt. In dieser Mittellage 50.2 des Schlüssels schaltet die zugehörige elektrische Steuereinheit die Zündung des Motors im Fahrzeug ein.

In der Mittellage 50.2 von Fig. 13 kommt es auf die kraftschlüssige Haltewirkung des Rastgesperres 70 nicht mehr an. Ein an der federnden Zunge 71 befindlicher radialer Vorsprung 75 greift zwar immer noch in die erwähnte Rastvertiefung 55 des Schlüssels 50 ein, doch liegt dieser Vorsprung 75, im Gegensatz zu Fig. 12, in Abstand von der für den Kraftschluss von Fig. 12 sorgenden Haltekante 76.

Ausgehend von Fig. 13 kann der Schlüssel 50 um eine weitere Hubstrecke 53 in die aus Fig. 14 ersichtliche Endlage 50.3 überführt werden. Dazu ist eine höhere Kraft

IPR2022-00412
Apple EX1053 Page 512

erforderlich, weil dem Einschieben 59 nicht nur die bisherige Rückstellfeder 40, sondern auch die zweite Rückstellfeder 40' entgegenwirken. Die Endlage 50.3 wird von einem weiteren Sensor 77 festgestellt. Dieser besteht im vorliegenden Fall ebenfalls aus einem Mikroschalter, dessen Betätiger 78 von der Unterkante 69 des Schlüsselprofils gedrückt wird. Auch dieser Schlüssel-Sensor 77 ist natürlich mit der elektrischen Steuereinheit verbunden. Gleichzeitig stellt die Steuereinheit in Fig. 14 den gedrückten Zustand des Klinken-Sensors 72 fest. Aufgrund ihrer Programmierung schaltet die Steuereinheit den Anlasser des Motors an. Der Motor startet. Dies kann zeitgesteuert erfolgen. Als weitere Bedingung kann die elektrische Steuerung das pedale Betätigen einer Fußbremse überwachen. Auf diese Weise kann ein versehentlicher Start des Motors verhindert werden, wenn die Fußbremse nicht getreten wird. Darüber hinaus wird aber im vorliegenden Fall die Endlage 50.3 des Schlüssels nur impulsweise erreicht, wie aus folgendem Umstand in Fig. 14 zu ersehen ist.

Der vorbeschriebene Halterarm 81 der Klinke 80 kann mit seinem Hakenende 87 sich in dem entsprechend breit bemessenen Randausbruch 89 des Schlüssels von seiner die Verriegelung bedingenden Schulter 88 axial entfernen. Trotz des Eingriffs der Klinke 80 in den Randausbruch 89 erweist sich diese Verriegelung 80 von Fig. 13 als ein „Richtgesperre", welches zwar das Herausziehen 57 des Schlüssels 50 aus der Mittellage 50.2 von Fig. 13 verhindert, aber ein tieferes Einschieben 59 des Schlüssels in die Endlage 50.3 gestattet. Es handelt sich um eine ähnliche Wirkung, die beim ersten Ausführungsbeispiel von gesonderten Mitteln 30, 31, 24 besorgt werden musste. In diesem zweiten Ausführungsbeispiel übernehmen die Haltemittel 81, 88, 89 der formschlüssigen Verriegelung 80 zugleich die Funktion dieses „Richtgesperres".

Der vorbeschriebene weitere Abwärtshub 53 des Schlüssels wird auch nicht von den Elementen des kraftschlüssigen Rastgesperres 70 behindert. Wie Fig. 14 zeigt, erlaubt die Größe der Rastaussparung 55 eine entsprechend ungestörte Verschiebung des radialen Vorsprungs 75 an der zugehörigen federnden Zunge 71. Der Freiraum bei 89 im Bereich der Klinke 80 einerseits und bei 55 im Bereich des Rastgesperres 70 andererseits erlauben es, dass die von den Rückstellfedern 40, 40' ausgeübte

IPR2022-00412
Apple EX1053 Page 513

Rückstellkraft 41 den Schlüssel 50 aus Fig. 14 wieder in die Mittellage 50.2 von Fig. 13 zurückführt. Die Mittellage 50.2 ist ja durch das wie ein „Sperrarm" wirkende Halteelement 81 der Klinke 80 gesichert; das Hakenende 87 hintergreift wieder die Schulter 88 vom Schlüssel 50. Es liegt dann wieder die im Zusammenhang mit Fig. 13 bereits beschriebene Stellung „Zündung" des Motors vor. Der vorausgehend in Fig. 14 gestartete Motor läuft in Fig. 13 weiter.

Um den Motor auszuschalten, braucht, ausgehend von der Mittellage 15.2 des Schlüssels 50 in Fig. 13 der Schlüssel 50 nur noch erneut, ein zweites Mal, in seine Endlage von Fig. 14 gedrückt zu werden. Es kommt dabei nicht darauf an, ob die Fußbremse dabei ebenfalls getreten oder nicht getreten wird. Stattdessen kann die elektrische Steuerung über einen Sensor den Bremskonkakt oder die Raddrehung vom Fahrzeug sensieren. Die elektrische Steuereinheit schaltet aber auch einen auf die Klinke 80 wirkenden Antrieb 48 gemäß Fig. 9 ein. Dieser besteht auch in diesem zweiten Ausführungsbeispiel aus einem Hubmagneten 48, der über einen Stößel 49 auf einen drehfest mit der Klinke 80 verbundenen Lösearm 83 einwirkt. Die Klinke 80 wird in die strichpunktiert in Fig. 9 verdeutlichte Entriegelungsstellung 80' überführt. Dann ist die Schulter 88 frei. Weil die Rückstellfeder 40 eine Rückstellkraft 41 ausübt, schiebt sie den Schlüssel 50 aus der Mittellage 50.2 von Fig. 13 bzw. 9 wieder in die Anfangslage 50.1 von Fig. 12 zurück. Dann ist der Formschluss beseitigt. Das Verriegelungsgesperre 80 ist gemäß Fig. 12 durch den beschriebenen Profilbereich 79 entriegelt. Es liegt wieder nur der Kraftschluss des Rastgesperres 70 vor. Die manuelle Entnahme 57 des Schlüssels 50 ist in Fig. 12 wieder ohne weiteres möglich. Beim Klinken-Sensor 72 befindet sich der Betätiger 73 wieder im umgedrückten Zustand.

Ausgehend von der Anfangslage 50.1 des Schlüssels 50 in Fig. 12 kann der Schlüssel 50 natürlich alternativ, durch erneutes zweistufiges Drücken 59, über die Mittellage 50.2 von Fig. 13, wo sich die Zündung von der Steuereinheit wieder einschaltet, die Endlage 50.3 gemäß Fig. 14 gebracht werden, wo der Motor gestartet wird. Eine Fehlbedienung ist ausgeschlossen.

IPR2022-00412
Apple EX1053 Page 514

Auch in diesem zweiten Ausführungsbeispiel kann der mit der Klinke 80 zusammenwirkende Hubmagnet 48 dazu genutzt werden, um einen „falschen Schlüssel" aus der Vorrichtung zu entfernen. Es könnten zunächst die Haltelage 50.1 von Fig. 12 und möglicherweise auch die Endlage 50.2 von Fig. 13 mit einem falschen Schlüssel erreicht sein. Spätestens dann identifiziert aber der Transponder 43 od. dgl. den „falschen Schlüssel". Daraufhin schaltet die elektrische Steuereinheit den Hubmagneten 48 ein, der über seinen Stößel 49 die Klinke 80 in ihre beschriebene Entriegelungsstellung 80' überführt. Die von den Rückstellfedern 40 ausgeübte Rückstellkraft 41 drückt dann den falschen Schlüssel in die Anfangslage 50.1 von Fig. 12 zurück. Der Motor konnte mit dem falschen Schlüssel nicht gestartet werden.

Sofern das Fahrzeug mit einem „Automatikgetriebe" versehen ist, muss bei der Schlüsselentnahme 57 in der Anfangsstellung 50.1 von Fig. 12 der Wählhebel auf den Stellungen „B" oder „N" stehen. Außerdem ist bei dieser Vorrichtung ebenso wie beim ersten Ausführungsbeispiel eine elektrische Lenkradverriegelung vorgesehen, die bei entnommenen Schlüssel für eine Verriegelung des Lenkrads sorgt. Befindet sich der richtige Schlüssel in der Aufnahme 11, der dann vom Transponder 43 festgestellt wird, so wird die Lenkradverriegelung unwirksam gesetzt. Außerdem ist ein nicht näher gezeigter Sensor im Bereich der Aufnahme 11 vorgesehen, welcher in beiden Ausführungsbeispielen eine Verriegelung des Lenkrads dann ausschließt, solange der Schlüssel 50 sich in einen seiner drei Hublagen 50.1, 50.2 oder 50.3 befindet. Erst wenn der Schlüssel 57 aus dem Gehäuse 10 ganz entnommen ist, wird die Lenkradverriegelung wirksam gesetzt. Ebenso wird in allen Fahrtstellungen eines Automatik-Getriebes eine Auswurfbewegung auf den in der Mittellage 50.2 befindlichen Schlüssel 50 der Schlüssel nicht freigegeben und die Lenkradsicherung nicht in ihre Verriegelungsposition überführt. So lassen sich leicht Fehlbedienungen verhindern.

Im Gehäuse kann eine aus Fig. 9 und 10 ersichtliche Beleuchtung 90 vorgesehen sein, die beim Öffnen der Tür für eine bestimmte Zeit aktiviert wird. Dann wird der Einführschlitz 13 beleuchtet und erleichtert das Einführen der Karte 50.

IPR2022-00412
Apple EX1053 Page 515

Bezugszeichenliste :

10	Gehäuse
11	Aufnahme
12	Kontur der Armatur
13	stirnseitige Öffnung von 11
14	Abdeckung von 11
14'	Abdeckklappe (Fig. 10)
14.1	Ausschubstellung von 14 (Fig. 1, 2)
14.2	Einschubstellung von 14 (Fig. 6 bis 7)
15	Abdeck-Druckfeder für 14
16	radiale Aussparung von 10 für 23
17	Blende für 13
18	axiales Führungsmittel bei 17, Steg
19	radiale Stützfläche für 23 von 10
20	Schieber
20.1	erste Axialposition von 20, Ausgangsposition (Fig. 1 bis 5)
20.2	zweite Axialposition von 20, Arbeitsposition (Fig. 6)
20.3	dritte Axialposition von 20, Endposition (Fig. 7)
21	Halteelement für 50, federnde Zunge
22	erster Endanschlag für 14, Halteelement für 50, federnder Vorsprung
23	Gegenvorsprung an 21
24	Schulter für 31, Nocken (Richtgesperre)
25	Axialansatz von 20
26	Innenbund in 25 für 40
27	Punktlinie, Verschiebungsweg von 24
28	herausragendes Teilstück von 50 (Fig. 5)
29	zweiter Endanschlag von 14 (Fig. 5)
30	Riegel, Klinke (Richtgesperre)
31	Sperrarm von 30 (Richtgesperre)

IPR2022-00412
Apple EX1053 Page 516

32	Lösearm von 30
33	Schwenklager von 30
34	Axialführung für 35 (Fig. 8)
35	Betätiger, Taster
36	Druckbetätigungspfeil zur Tasterbetätigung für 35 (Fig. 8)
37	Rückstellfeder für 35
38	Schriftfeld-Teil von 35 für 46
38‘	Schriftfeld-Rest von 35 für 46‘
39	Lichttrennwand an 35 (Fig. 8)
40	Rückstellfeder für 20 (Fig. 1 bis 8) bzw. für 50 (Fig. 9 bis 14)
40‘	weitere Rückfestellfeder für 50 (Fig. 9 bis 14)
41	Pfeil der axialen Rückstellkraft von 20 bzw. 50, axiale Federbelastung
42	Endanschlag an 10 für 20 (Fig. 5)
43	Transponder der elektronischen Steuereinheit
44	Sensor für 35 (Fig. 2, 8)
45	Gehäusehülse für 25
46	Diode für „Start“ in 35 (Fig. 8)
46‘	Diode für „Stop“ in 35 (Fig. 8)
47	Sensor für 50.3
48	Antrieb, Hubmagnet
49	Stößel von 48
50	elektronischer Schlüssel
50.0	Berührungslage von 50 (Fig. 1, 2)
50.1	erste axiale Hublage von 50, Anfangslage (Fig. 5)
50.2	zweite axiale Hublage von 50, Mittellage (Fig. 6)
50.3	dritte axiale Hublage von 50, Endlage (Fig. 7)
51	erste Hubstrecke von 50 (Fig. 5)
52	zweite Hubstrecke von 50 (Fig. 6)
53	dritte Hubstrecke von 50 (Fig. 7)
54	axiales Führungsmittel an 50, Längsnut
55	Halteelement, Rastvertiefung
56	herausragendes Endstück von 50 bei 50.2 (Fig. 6)
57	Pfeil des Rückschubs, Herausziehbewegung von 50 aus 11

58 Vorderstück von 50
59 Pfeil der Einschubbewegung von 50 in 11
60 Dämpfungseinrichtung für 20, Dämpfungsrad
61 Drehachse von 60
62 Stirnrad von 60
63 Zahnstange für 62
64 Schaltnocken für 47 (Fig. 2)
65 Steckkontakt an 10
66 Leiterplatte
67 Zwischenboden (Fig. 3)
68 Kartenumriss von 50 (Fig. 11), Schlüsselprofil
69 Unterkante von 50
70 kraftschlüssiges Rastgesperre
71 Halteelement von 70, federnde Zunge
72 Klinken-Sensor
73 Betätiger von 72
74 Stößel für 40
74' Stößel für 40'
75 federnder Vorsprung an 71
76 Haltekante von 55 für 50 (Fig. 12)
77 Schlüssel-Sensor
78 Betätiger von 77
79 Profilbereich von 68 für Abstützung von 81
80 Richtgesperre, Klinke (Verriegelungsstellung)
80' Entriegelungsstellung von 80
81 Halteelement von 80, Sperrarm
82 Stellarm von 80
83 Lösearm von 80
84 Schwenklager für 80
85 Klinken-Federbelastung
86 Rückschwenk-Kraft von 85 auf 80
87 Hakenende von 81
88 Schulter für 87 von 80

89 Randausbruch von 68 für 87

90 Beleuchtung in 11 (Fig. 10)

Patentansprüche :

1.) Vorrichtung zum Starten eines Fahrzeug-Motors mittels eines elektronischen Schlüssels (50), der gegebenenfalls ein Scheckkarten-Format aufweist,

mit einer zum Einstecken (59) des Schlüssels (50) dienenden Aufnahme (11) im Fahrzeug,

wobei der in der Aufnahme (11) eingesteckte Schlüssel (50) manuell in verschiedene Schlüssellagen überführbar ist

und die Schlüssellagen von Sensoren einer elektronischen Steuereinheit überwacht und zur Steuerung von verschiedenen Funktionen des Motors und gegebenenfalls weiterer Zusatzgeräte im Kraftfahrzeug, wie einem Radio, genutzt werden,

dadurch gekennzeichnet ,

dass der eingesteckte Schlüssel (50) in der Aufnahme (11) unverdrehbar und mindestens zwischen drei zueinander axial versetzten Hublagen (50.1, 50.2, 50.3) längsverschiebbar (51, 52, 53) ist, nämlich,

beim anfänglichen Einstecken (59), zunächst in eine den Schlüssel (50) im vorderen Bereich der Aufnahme (11) nur kraftschlüssig sichernden Anfangslage (50.1),

dann, beim Weiterschieben (59) um eine erste Hubstrecke (52), in eine den Schlüssel (50) im mittleren Bereich der Aufnahme (11) formschlüssig sichernden Mittellage (50.2),

IPR2022-00412
Apple EX1053 Page 520

welche zwar ein manuelles Herausziehen (57) des Schlüssels (50) aus der Aufnahme (11) verhindert, aber ein Weiterschieben (59) des Schlüssels (50) erlaubt,

und schließlich beim Weiterschieben (59) um eine zweite Hubstrecke (53) in eine den Schlüssel (50) im hinteren Bereich der Aufnahme (11) positionierende Endlage (50.3),

dass der Schlüssel (50) mindestens in seiner Mittel- und Endlage (50.2, 50.3) in Richtung seiner Anfangslage (50.1) entweder unmittelbar oder mittelbar (20) von einer Rückstellfeder (40) axial federbelastet (41) ist, wobei die Sensoren der Steuereinheit mindestens einige der drei Schlüssel-Hublagen (50.1, 50.2, 50.3) überwachen.

2.) Vorrichtung nach Anspruch 1, dadurch gekennzeichnet, dass wenigstens ein manueller und/oder pedaler Betätiger (35) im Fahrzeug angeordnet ist und mit der Steuereinheit in Wirkverbindung steht

und dass eine Betätigung des Betätigers (35) die Auswahl der verschiedenen Funktionen des Fahrzeugs mitbestimmt.

3.) Vorrichtung nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass der Schlüssel (50) beim Weiterschieben (59) aus der Mittellage (50.2) seine Endlage (50.3) nur impulsweise erreicht

und dass - nach Beendigung des manuellen Einschubdrucks - die Rückstellfeder (40) den Schlüssel (50) selbsttätig wieder in die Mittellage (50.2) oder die Anfangslage (50.1) zurückschiebt (75).

IPR2022-00412
Apple EX1053 Page 521

4.) Vorrichtung nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass die Aufnahme (11) sowohl ein den Kraftschluss erzeugendes Rastgesperre (21, 22, 55; 70) für den eingesteckten Schlüssel (50) als auch ein mittelbar (20) oder unmittelbar mit dem Schlüssel (50) zusammenwirkendes Richtgesperre (24, 30, 31; 80) besitzt,

dass das Rastgesperre (21, 22, 55; 70) mindestens in der Anfangslage (50.1), aber das Richtgesperre (24, 30, 31; 80) sowohl in der Mittellage (50.2) als auch in der Endlage (50.3) des Schlüssels (50) wirksam sind

und dass bei wirksamem Richtgesperre (24, 30, 31; 80) das Weiterschieben (59) des Schlüssels (50) aus der Mittellage (50.2) in die Endlage (50.3) und das rückstellfederbedingte Zurückschieben (57) des Schlüssels (50) aus der Endlage (50.3) in die Mittellage (50.2) zwar möglich sind,

aber ein Zurückschieben (57) des Schlüssels (50) aus der Mittellage (50.2) in die Anfangslage (50.1) verhindert ist.

5.) Vorrichtung nach Anspruch 4, dadurch gekennzeichnet, dass beim Einschieben (59) des Schlüssels (50) in die Anfangslage (50.1) das Rastgesperre (21, 22, 50; 70) und beim Einschieben (59) in die Mittellage (50.2) das Richtgesperre (24, 30, 31; 80) selbsttätig wirksam setzbar sind

und dass die Steuereinheit auf ein einmaliges oder mehrmaliges Eindrücken (59) des Schlüssels (50) zwischen der Mittellage (50.2) in die Endlage (50.3) anspricht und das Richtgesperre (24, 30, 31; 80) solange unwirksam setzt, bis die Rückstellfeder-Kraft (41) den Schlüssel (50) in die Anfangslage (50.1) zurückgeschoben (57) hat.

6.) Vorrichtung nach Anspruch 5, dadurch gekennzeichnet,

dass das Richtgesperre einen seinerseits federbelasteten (85) Riegel (30; 80) aufweist, der in den axialen Weg (27) einer entweder unmittelbar oder mittelbar (20) mit dem Schlüssel (50) mitverschieblichen Schulter (24; 88) hineinragt und die Schulter (24; 88) in der Endlage (50.3) des Schlüssels (50) hintergreift

und dass die Steuereinheit im Ansteuerungsfall den Riegel (30; 80) gegen seine Riegel-Federbelastung (86) aus dem axialen Weg der Schulter (24; 88) herausbewegt.

7.) Vorrichtung nach Anspruch 6, dadurch gekennzeichnet, dass der Riegel aus einer federbelasteten Klinke (30; 80) besteht, wobei die Klinke (30; 80) außer einem mit der Schulter (21; 88) zusammenwirkenden Sperrarm (31; 81) einen damit drehfesten Lösearm (32) besitzt,

und dass der Lösearm (32; 83) mit einem Antrieb (48), wie einem elektrischen Hubmagneten (48), verbunden ist, der von der elektrischen Steuereinheit gesteuert wird.

8.) Vorrichtung nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass in der Aufnahme (11) elektronische Identifikationsmittel für den Schlüssel (50) angeordnet sind, die mit der elektrischen Steuereinheit in Wirkverbindung stehen,

und dass bei Ermittlung eines falschen Schlüssels (50) der Antrieb (48) für die Klinke (30; 80) wirksamgesetzt wird und den Riegel freigibt,

wodurch der falsche Schlüssel (50) von der Rückstellfederkraft (41) in seine Anfangslage (50.1) in der Aufnahme (11) zurückgeschoben wird.

9.) Vorrichtung nach Anspruch 8, dadurch gekennzeichnet, dass die elektronischen Identifikationsmittel aus einem Transponder (48) bestehen.

10.) Vorrichtung nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass die kraftschlüssigen Halteelemente (21; 81) des Rastgesperres einerseits aus einem federnden Glied (22) im Bereich der Aufnahme (11) und andererseits aus einer Rastvertiefung (59) am Schlüssel (50) bestehen.

11.) Vorrichtung nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, dass der Schlüssel (50) die Umrissform (68) einer Scheckkarte hat.

12.) Vorrichtung nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, dass das Rastgesperre (70) und Richtgesperre (80) ortsfest in einem die Aufnahme (11) umschließenden Gehäuse (10) angeordnet sind,

dass nicht nur die Rastvertiefung (55) für das Rastgesperre (70), sondern auch die Schulter (88) des Richtgesperres (80) unmittelbar am Umrissprofil (68) des Schlüssels (50) sich befinden

und dass die Verriegelungs-Elemente (81) des Richtgesperres (80) zugleich die formschlüssigen Halteelemente für den Schlüssel (59) sind.

13.) Vorrichtung nach einem der Ansprüche 6 bis 12, dadurch gekennzeichnet, dass die Klinke (80) des Richtgesperres einen drehfest mit dem Sperr- und Lösearm (81, 83) ausgebildeten Stellarm (82) aufweist

und der Stellarm (82) auf einen Klinken-Sensor (72) einwirkt.

IPR2022-00412
Apple EX1053 Page 524

14.) Vorrichtung nach Anspruch 13, dadurch gekennzeichnet, dass die Sperrstellung der Klinke (80) durch die Klinken-Federbelastung (85) und gegebenenfalls einen Drehanschlag bestimmt ist,

dass die Sperrstellung sowohl bei herausgezogenem Schlüssel (50), also bei leerer Aufnahme (11), als auch bei einem in der Mittellage (50.2) und in der Endlage (50.3) befindlichen Schlüssel (50) vorliegt

und dass der Klinken-Sensor (72) vom Stellarm (82) zwar in der Sperrstellung der Klinke (80) betätigt wird,

aber in der Anfangslage (50.1) des Schlüssels (50) die Klinke (80) von einem Profilabschnitt (79) des Schlüssel-Umrissprofils (68) aus ihrer Sperrstellung gegen die Klinken-Federbelastung (86) verschwenkt (80') ist und den Klinken-Sensor (72) freigibt.

15.) Vorrichtung nach Anspruch 14, dadurch gekennzeichnet, dass die Aufnahme (11) außer dem Klinken-Sensor (72) einen ebenfalls mit der Steuereinheit in Verbindung stehenden Schlüssel-Sensor (77) besitzt, der die Endlage (50.3) des Schlüssels (50) überwacht.

16.) Vorrichtung nach einem der Ansprüche 1 bis 15, dadurch gekennzeichnet, dass die auf den Schlüssel (50) wirkende axiale Rückstellkraft (41) sich in Abhängigkeit von dessen Hublage (50.1, 50.2, 50.3) in der Aufnahme (11) stufenartig verändert

und dass die Rückstellkraft (41) in der Anfangslage (50.1) des Schlüssels (50) geringer als in der Mittellage (50.2) und der Endlage (50.3) ist.

IPR2022-00412
Apple EX1053 Page 525

17.) Vorrichtung nach einem der Ansprüche 1 bis 16, dadurch gekennzeichnet, dass der zur Auswahl verschiedener Funktionen im Fahrzeug dienende manuelle oder pedale Betätiger (35) zwar in der Mittellage (50.2) des Schlüssels wirksam, aber in allen übrigen Lagen (50.0, 50.1, 50.3) des Schlüssels (50) unwirksam ist.

18.) Vorrichtung nach einem der Ansprüche 1 bis 11 und 17 mit einer Aufnahme (11), deren Öffnung (13) normalerweise von einer federnden (15) Abdeckung (14) verschlossen (14.1) ist,

wobei die Abdeckung (14) beim Einstecken (59) vom Schlüssel (50) gegen die Abdeck-Federbelastung (15) weggedrückt (14.2) wird,

d a d u r c h g e k e n n z e i c h n e t ,

dass die Abdeckung (14) Bestandteil eines im Gehäuse (10) der Aufnahme (11) axial beweglichen Schiebers (20) ist,

dass der Schieber (20) beim Einstecken (59) das Vorderstück (48) des Schlüssels (50) aufnimmt und der Schieber (20) sowohl die kraftschlüssig als auch formschlüssig auf den Schlüssel (50) einwirkenden Haltemittel (21, 22, 55) besitzt, wobei diese Haltemittel den Schlüssel (50) im Schieber (20) sichern,

dass der Schieber (20) durch die Axialbewegung (59) des Schlüssels (50) in verschiedene Axialpositionen (20.1, 20.2, 20.3) überführbar ist, welche die verschiedenen Hublagen (50.1, 50.2, 50.3) des Schlüssels (50) bestimmen,

und dass der Schieber (20) axial federbelastet (40) ist und dadurch auf den eingesteckten Schlüssel (50) ausgeübte Rückstellkraft (41) erzeugt,

und dass der Schieber (20) in seiner die Mittellage (50.2) des Schlüssels (50) bestimmenden mittleren Axialposition (50.2) von einem federnden Riegel (30) eines Richtgesperres festgehalten wird und dieses Richtgesperre mittelbar, über den Schieber (20), auf den Schlüssel (50) wirkt.

19.) Vorrichtung nach Anspruch 18, dadurch gekennzeichnet, dass der Schieber (20) sowohl in der Anfangslage (50.1) des eingesteckten Schlüssels (50) als auch bei herausgezogenem Schlüssel sich in der gleichen Ausgangsposition (20.1) im Gehäuse (10) der Aufnahme (11) befindet,

und dass die Ausgangsposition (50.1) durch die auf den Schieber (20) wirkende axiale Federkraft (41) einerseits und einen Endanschlag (42) im Gehäuse (10) der Aufnahme (11) andererseits bestimmt ist.

20.) Vorrichtung nach Anspruch 19, dadurch gekennzeichnet, dass die Abdeckung (14) für die Öffnung (13) der Aufnahme (11) ihrerseits zwischen zwei Stellungen (14.1, 14.2) im Schieber (20) axial verschieblich ist,

dass diese beiden Stellungen (14.1, 14.2) durch einen vorderen und einen hinteren Endanschlag (22, 29) im Schieber (20) bestimmt sind,

dass die Abdeck-Federbelastung (15) bestrebt ist, die Abdeckung (14) axial gegen den vorderen Endanschlag (22) zu drücken,

und dass der vordere Endanschlag (22) und die Abdeck-Federbelastung (15) die bei herausgezogenem Schlüssel (50) sich ergebende abdeckwirksame Ausschubstellung (14.1) der Abdeckung (14) an der Öffnung (13) bestimmen.

21.) Vorrichtung nach Anspruch 20, dadurch gekennzeichnet, dass bei eingestecktem Schlüssel (50) die Abdeckung (14) sich in einer durch den

hinteren Endanschlag (29) am Schieber (20) bestimmten Einschubstellung (14.2) befindet

und dass diese Einschubstellung (14.2) der Abdeckung (14) in allen drei axialen Hublagen des Schlüssels (50) vorliegt.

22.) Vorrichtung nach einem der Ansprüche 18 bis 21, dadurch gekennzeichnet, dass die gleichen Halteelemente (21, 22, 55), welche die kraftschlüssige Verbindung zwischen dem Schlüssel (50) und dem Schieber (20) erzeugen, auch bei der formschlüssige Verbindung zwischen dem Schlüssel (50) und dem Schieber (20) beteiligt sind.

23.) Vorrichtung nach Anspruch 22, dadurch gekennzeichnet, dass die am Schieber (20) befindlichen kraftschlüssigen Halteelemente (21, 22) einen federnden Vorsprung (22) aufweisen

dass dem Vorsprung (22) ein Gegenvorsprung (23) auf seiner dem Gehäuse (10) der Aufnahme (11) zugekehrten Rückseite zugeordnet ist,

dass dieser Gegenvorsprung (23) in der die Haltelage (50.1) des Schlüssels (50) kennzeichenden Ausgangsposition (20.1) des Schiebers (20) mit einer Aussparung (16) im Gehäuse (10) radial ausgerichtet ist, in welchen der Gegenvorsprung (23) federnd ausweicht, wenn der Schlüssel (50) eingesteckt (59) wird,

und dass dem Gegenvorsprung (23) eine radiale Stützfläche (19) im Gehäuse (10) zugeordnet ist, die das federnde Glied (22) radial versteift, wenn der Schieber (20) vom Schlüssel (50) aus seiner Ausgangsposition (20.1) in eine der tiefer gelegenen Axialpositionen (20.2, 20.3) weiterbewegt wird.

IPR2022-00412
Apple EX1053 Page 528

24.) Vorrichtung nach einem der Ansprüche 17 bis 23, dadurch gekennzeichnet, dass der axialbewegliche Schieber (20) ein mit einer Dämpfungseinrichtung (60) versehen ist,

und dass die Dämpfungseinrichtung (60) die federbedingte (40) axiale Rückbewegung (57) des im Schieber (20) aufgenommenen Schlüssels (50) aus dessen Endlage (50.3), über die Mittellage (50.2), bis zur Anfangslage (50.1) bremst.

25.) Vorrichtung nach einem der Ansprüche 1 bis 24, dadurch gekennzeichnet, dass die zur Unterscheidung der ausgewählten Funktion dienende Steuereinheit auch auf Betätigung bzw. Nichtbetätigung weiterer Steuerglieder im Fahrzeug anspricht, wie eine Fußbremse.

26.) Vorrichtung nach einem der Ansprüche 1 bis 24, dadurch gekennzeichnet, dass die zur Unterscheidung der ausgewählten Funktionen dienende Steuereinheit auf eine Nicht-Betätigung weiterer Steuerglieder im Fahrzeug anspricht.

27.) Vorrichtung nach einem der Ansprüche 1 bis 26, dadurch gekennzeichnet, dass der für die verschiedenen Funktionen im Kraftfahrzeug dienende Betätiger einen Taster (35) umfasst

und dass die elektrische Steuereinheit die Anzahl und/oder die Reihenfolge der verschiedenen Betätigungen (36) unterscheidet und dementsprechend die ausgewählten Funktionen im Kraftfahrzeug auslöst.

28.) Vorrichtung nach einem der Ansprüche 1 bis 27, dadurch gekennzeichnet, dass zum unverdrehbaren Einstecken axiale Führungsmittel (18, 54) zwischen dem Schlüssel (50) einerseits und der Aufnahme (11) andererseits vorgesehen sind.

29.) Vorrichtung nach Anspruch 28, dadurch gekennzeichnet, dass die zur Aufnahme (11) gehörenden axialen Führungsmittel (18) in einer die Öffnung (13) der Aufnahme umschließenden Blende (17) angeordnet sind

und dass im Bereich der am Schlüssel (50) vorgesehenen Führungsmittel (54) auch die Angriffsstellen (55) für die kraftschlüssig und/oder formschlüssig wirksamen Halteelemente (21, 22, 23) des Rast- und/oder Richtgesperres angeordnet sind.

IPR2022-00412
Apple EX1053 Page 530

GEÄNDERTE ANSPRÜCHE

[beim Internationalen Büro am 09. Januar 2001 (09.01.01) eingegangen; ursprüngliche Ansprüche 1-29 durch neue Ansprüche 1-20 ersetzt (8 Seiten)]

1.) Vorrichtung zum Starten eines Fahrzeug-Motors mittels eines elektronischen Schlüssels (50), der gegebenenfalls ein Scheckkarten-Format aufweist,

mit einer zum Einstecken (59) des Schlüssels (50) dienenden Aufnahme (11) im Fahrzeug,

wobei der in der Aufnahme (11) eingesteckte Schlüssel (50) unverdrehbar und mindestens zwischen drei zueinander axial versetzten Hublagen (50.1, 50.2, 50.3) längsverschiebbar (51, 52, 53) ist

wobei der Schlüssel (50) in seiner Endlage (50.3) in Richtung seiner Anfangslage (50.1) entweder unmittelbar oder mittelbar von einer Rückstellfeder (40) axial federbelastet (41) ist und

einige der drei Schlüssel-Hublagen (50.1, 50.2, 50.3) von Sensoren einer Steuereinheit überwacht und zur Steuerung von verschiedenen Funktionen des Motors genutzt werden,

d a d u r c h g e k e n n z e i c h n e t ,

dass der Schlüssel (50) auch in seiner Mittellage (50.2) in Richtung seiner Anfangslage (50.1) von einer Rückstellfeder (40) axial federbelastet (41) ist und

beim Einschieben (59) des Schlüssels (50) in die Anfangslage (50.1) ein Rastgesperre (21, 22; 50; 70) und beim Einschieben (59) in die Mittellage (50.2) ein mit dem Schlüssel (50) mittelbar (20) oder unmittelbar zusammenwirkendes Richtgesperre (24; 30, 31; 80) selbsttätig wirksam setzbar sind und

IPR2022-00412
Apple EX1053 Page 531

dass die Steuereinheit auf ein einmaliges oder mehrmaliges Eindrücken (59) des Schlüssels (50) zwischen der Mittellage (50.2) in die Endlage (50.3) anspricht und das Richtgesperre (24; 30, 31; 80) solange unwirksam setzt, bis die Rückstellfederkraft (41) den Schlüssel (50) selbsttätig in die Anfangslage (50.1) zurückgeschoben (57) hat.

2.) Vorrichtung nach Anspruch 1, dadurch gekennzeichnet,

dass das Richtgesperre einen seinerseits federbelasteten (85) Riegel (30; 80) aufweist, der in den axialen Weg (27) einer entweder unmittelbar oder mittelbar (20) mit dem Schlüssel (50) mitverschieblichen Schulter (24; 88) hineinragt und die Schulter (24; 88) in der Endlage (50.3) des Schlüssels (50) hintergreift

und dass die Steuereinheit im Ansteuerungsfall den Riegel (30; 80) gegen seine Riegel-Federbelastung (86) aus dem axialen Weg der Schulter (24; 88) herausbewegt.

3.) Vorrichtung nach Anspruch 2, dadurch gekennzeichnet, dass der Riegel aus einer federbelasteten Klinke (30; 80) besteht, wobei die Klinke (30; 80) außer einem mit der Schulter (21; 88) zusammenwirkenden Sperrarm (31; 81) einen damit drehfesten Lösearm (32) besitzt,

und dass der Lösearm (32; 83) mit einem Antrieb (48), wie einem elektrischen Hubmagneten (48), verbunden ist, der von der elektrischen Steuereinheit gesteuert wird.

4.) Vorrichtung nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass in der Aufnahme (11) elektronische Identifikationsmittel für den Schlüssel

IPR2022-00412
Apple EX1053 Page 532

(50) angeordnet sind, die mit der elektrischen Steuereinheit in Wirkverbindung stehen,

und dass bei Ermittlung eines falschen Schlüssels (50) der Antrieb (48) für die Klinke (30; 80) wirksamgesetzt wird und den Riegel freigibt,

wodurch der falsche Schlüssel (50) von der Rückstellfederkraft (41) in seine Anfangslage (50.1) in der Aufnahme (11) zurückgeschoben wird.

5.) Vorrichtung nach Anspruch 4, dadurch gekennzeichnet, dass die elektronischen Identifikationsmittel aus einem Transponder (43) bestehen.

6.) Vorrichtung nach einem der Ansprüche 2 bis 5, dadurch gekennzeichnet, dass die Klinke (80) des Richtgesperres einen drehfest mit dem Sperr- und Lösearm (81, 83) ausgebildeten Stellarm (82) aufweist

und der Stellarm (82) auf einen Klinken-Sensor (72) einwirkt.

7.) Vorrichtung nach Anspruch 6, dadurch gekennzeichnet, dass die Sperrstellung der Klinke (80) durch die Klinken-Federbelastung (85) und gegebenenfalls einen Drehanschlag bestimmt ist,

dass die Sperrstellung sowohl bei herausgezogenem Schlüssel (50), also bei leerer Aufnahme (11), als auch bei einem in der Mittellage (50.2) und in der Endlage (50.3) befindlichen Schlüssel (50) vorliegt

und dass der Klinken-Sensor (72) vom Stellarm (82) zwar in der Sperrstellung der Klinke (80) betätigt wird,

IPR2022-00412
Apple EX1053 Page 533

aber in der Anfangslage (50.1) des Schlüssels (50) die Klinke (80) von einem Profilabschnitt (79) des Schlüssel-Umrissprofils (68) aus ihrer Sperrstellung gegen die Klinken-Federbelastung (86) verschwenkt (80') ist und den Klinken-Sensor (72) freigibt.

8.) Vorrichtung nach Anspruch 7, dadurch gekennzeichnet, dass die Aufnahme (11) außer dem Klinken-Sensor (72) einen ebenfalls mit der Steuereinheit in Verbindung stehenden Schlüssel-Sensor (77) besitzt, der die Endlage (50.3) des Schlüssels (50) überwacht.

9.) Vorrichtung nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass die auf den Schlüssel (50) wirkende axiale Rückstellkraft (41) sich in Abhängigkeit von dessen Hublage (50.1, 50.2, 50.3) in der Aufnahme (11) stufenartig verändert

und dass die Rückstellkraft (41) in der Anfangslage (50.1) des Schlüssels (50) geringer als in der Mittellage (50.2) und der Endlage (50.3) ist.

10.) Vorrichtung nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass der zur Auswahl verschiedener Funktionen im Fahrzeug dienende manuelle oder pedale Betätiger (35) zwar in der Mittellage (50.2) des Schlüssels wirksam, aber in allen übrigen Lagen (50.0, 50.1, 50.3) des Schlüssels (50) unwirksam ist.

11.) Vorrichtung nach einem der Ansprüche 1 bis 5 und 10 mit einer Aufnahme (11), deren Öffnung (13) normalerweise von einer federnden (15) Abdeckung (14) verschlossen (14.1) ist,

IPR2022-00412
Apple EX1053 Page 534

wobei die Abdeckung (14) beim Einstecken (59) vom Schlüssel (50) gegen die Abdeck-Federbelastung (15) weggedrückt (14.2) wird,

d a d u r c h g e k e n n z e i c h n e t ,

dass die Abdeckung (14) Bestandteil eines im Gehäuse (10) der Aufnahme (11) axial beweglichen Schiebers (20) ist,

dass der Schieber (20) beim Einstecken (59) das Vorderstück (48) des Schlüssels (50) aufnimmt und der Schieber (20) sowohl die kraftschlüssig als auch formschlüssig auf den Schlüssel (50) einwirkenden Haltemittel (21, 22, 55) besitzt, wobei diese Haltemittel den Schlüssel (50) im Schieber (20) sichern,

dass der Schieber (20) durch die Axialbewegung (59) des Schlüssels (50) in verschiedene Axialpositionen (20.1, 20.2, 20.3) überführbar ist, welche die verschiedenen Hublagen (50.1, 50.2, 50.3) des Schlüssels (50) bestimmen,

und dass der Schieber (20) axial federbelastet (40) ist und dadurch auf den eingesteckten Schlüssel (50) ausgeübte Rückstellkraft (41) erzeugt,

und dass der Schieber (20) in seiner die Mittellage (50.2) des Schlüssels (50) bestimmenden mittleren Axialposition (50.2) von einem federnden Riegel (30) eines Richtgesperres festgehalten wird und dieses Richtgesperre mittelbar, über den Schieber (20), auf den Schlüssel (50) wirkt.

12.) Vorrichtung nach Anspruch 11, dadurch gekennzeichnet, dass der Schieber (20) sowohl in der Anfangslage (50.1) des eingesteckten Schlüssels (50) als auch bei herausgezogenem Schlüssel sich in der gleichen Ausgangsposition (20.1) im Gehäuse (10) der Aufnahme (11) befindet,

IPR2022-00412
Apple EX1053 Page 535

und dass die Ausgangsposition (50.1) durch die auf den Schieber (20) wirkende axiale Federkraft (41) einerseits und einen Endanschlag (42) im Gehäuse (10) der Aufnahme (11) andererseits bestimmt ist.

13.) Vorrichtung nach Anspruch 12, dadurch gekennzeichnet, dass die Abdeckung (14) für die Öffnung (13) der Aufnahme (11) ihrerseits zwischen zwei Stellungen (14.1, 14.2) im Schieber (20) axial verschieblich ist,

dass diese beiden Stellungen (14.1, 14.2) durch einen vorderen und einen hinteren Endanschlag (22, 29) im Schieber (20) bestimmt sind,

dass die Abdeck-Federbelastung (15) bestrebt ist, die Abdeckung (14) axial gegen den vorderen Endanschlag (22) zu drücken,

und dass der vordere Endanschlag (22) und die Abdeck-Federbelastung (15) die bei herausgezogenem Schlüssel (50) sich ergebende abdeckwirksame Ausschubstellung (14.1) der Abdeckung (14) an der Öffnung (13) bestimmen.

14.) Vorrichtung nach Anspruch 13, dadurch gekennzeichnet, dass bei eingestecktem Schlüssel (50) die Abdeckung (14) sich in einer durch den hinteren Endanschlag (29) am Schieber (20) bestimmten Einschubstellung (14.2) befindet

und dass diese Einschubstellung (14.2) der Abdeckung (14) in allen drei axialen Hublagen des Schlüssels (50) vorliegt.

15.) Vorrichtung nach einem der Ansprüche 11 bis 14, dadurch gekennzeichnet, dass die gleichen Halteelemente (21, 22, 55), welche die kraftschlüssige Verbindung zwischen dem Schlüssel (50) und dem Schieber (20) erzeugen,

IPR2022-00412
Apple EX1053 Page 536

auch bei der formschlüssige Verbindung zwischen dem Schlüssel (50) und dem Schieber (20) beteiligt sind.

16.) Vorrichtung nach Anspruch 15, dadurch gekennzeichnet, dass die am Schieber (20) befindlichen kraftschlüssigen Halteelemente (21, 22) einen federnden Vorsprung (22) aufweisen

dass dem Vorsprung (22) ein Gegenvorsprung (23) auf seiner dem Gehäuse (10) der Aufnahme (11) zugekehrten Rückseite zugeordnet ist,

dass dieser Gegenvorsprung (23) in der die Haltelage (50.1) des Schlüssels (50) kennzeichenden Ausgangsposition (20.1) des Schiebers (20) mit einer Aussparung (16) im Gehäuse (10) radial ausgerichtet ist, in welchen der Gegenvorsprung (23) federnd ausweicht, wenn der Schlüssel (50) eingesteckt (59) wird,

und dass dem Gegenvorsprung (23) eine radiale Stützfläche (19) im Gehäuse (10) zugeordnet ist, die das federnde Glied (22) radial versteift, wenn der Schieber (20) vom Schlüssel (50) aus seiner Ausgangsposition (20.1) in eine der tiefer gelegenen Axialpositionen (20.2, 20.3) weiterbewegt wird.

17.) Vorrichtung nach einem der Ansprüche 10 bis 16, dadurch gekennzeichnet, dass der axialbewegliche Schieber (20) ein mit einer Dämpfungseinrichtung (60) versehen ist,

und dass die Dämpfungseinrichtung (60) die federbedingte (40) axiale Rückbewegung (57) des im Schieber (20) aufgenommenen Schlüssels (50) aus dessen Endlage (50.3), über die Mittellage (50.2), bis zur Anfangslage (50.1) bremst.

IPR2022-00412
Apple EX1053 Page 537

18.) Vorrichtung nach einem der Ansprüche 1 bis 17, dadurch gekennzeichnet, dass die zur Unterscheidung der ausgewählten Funktion dienende Steuereinheit auch auf Betätigung bzw. Nichtbetätigung weiterer Steuerglieder im Fahrzeug anspricht, wie eine Fußbremse.

19.) Vorrichtung nach einem der Ansprüche 1 bis 18, dadurch gekennzeichnet, dass die zur Unterscheidung der ausgewählten Funktionen dienende Steuereinheit auf eine Nicht-Betätigung weiterer Steuerglieder im Fahrzeug anspricht.

20.) Vorrichtung nach einem der Ansprüche 1 bis 19, dadurch gekennzeichnet, dass der für die verschiedenen Funktionen im Kraftfahrzeug dienende Betätiger einen Taster (35) umfasst

und dass die elektrische Steuereinheit die Anzahl und/oder die Reihenfolge der verschiedenen Betätigungen (36) unterscheidet und dementsprechend die ausgewählten Funktionen im Kraftfahrzeug auslöst.

IPR2022-00412
Apple EX1053 Page 538

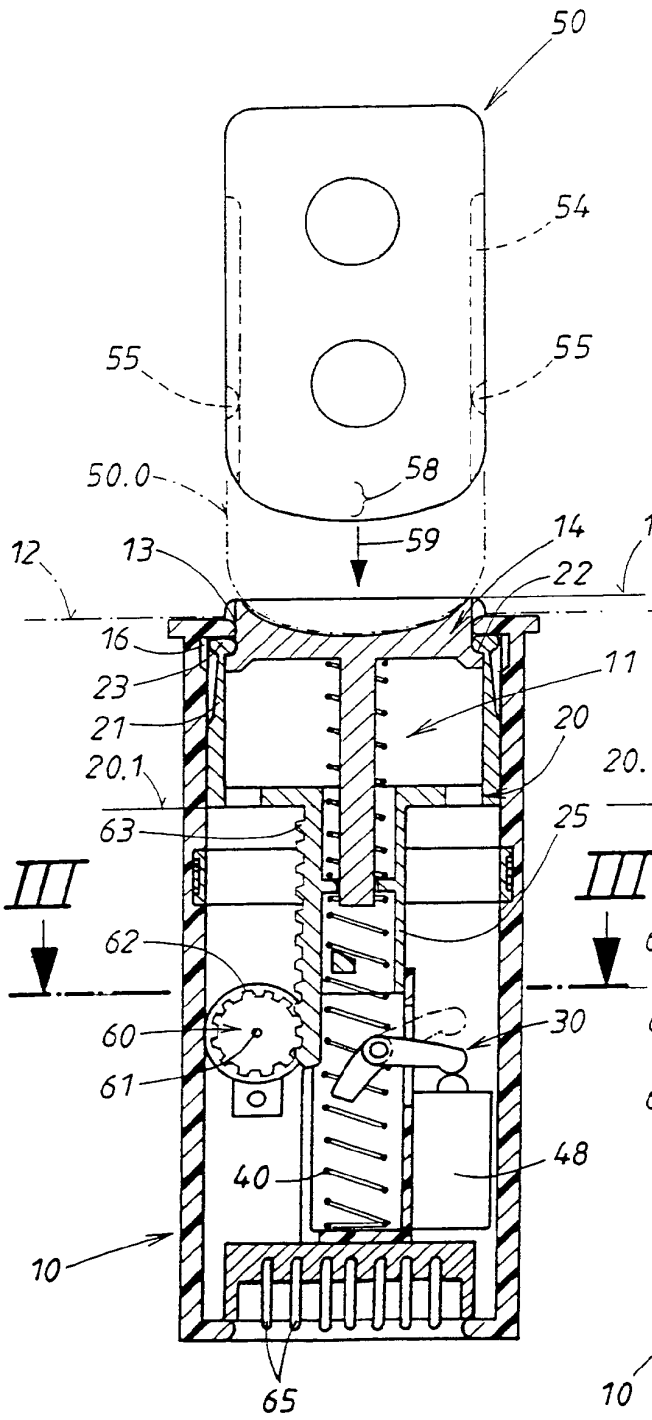

50
54
55
55
50.0
58
59
12
13
14
14.1
22
16
23
21
20.1
63
III
62
60
61
11
20
25
30
48
40
10
65

FIG. 1

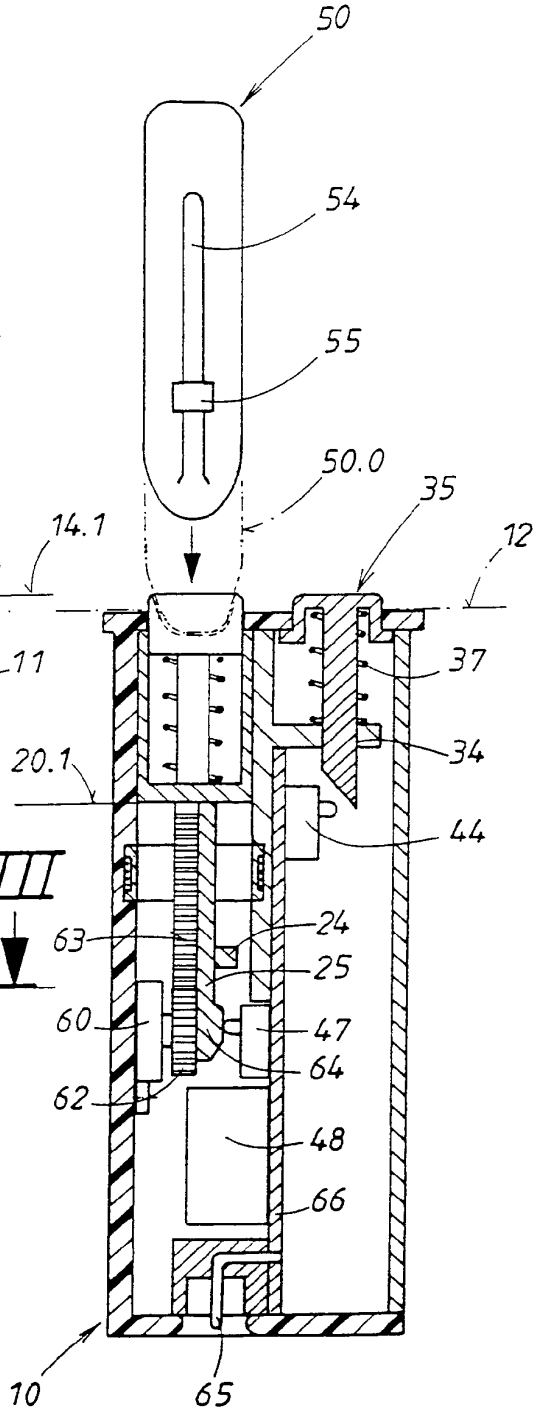

50
54
55
50.0
35
12
37
34
20.1
44
III
63
24
25
60
47
64
62
48
66
10
65

FIG. 2

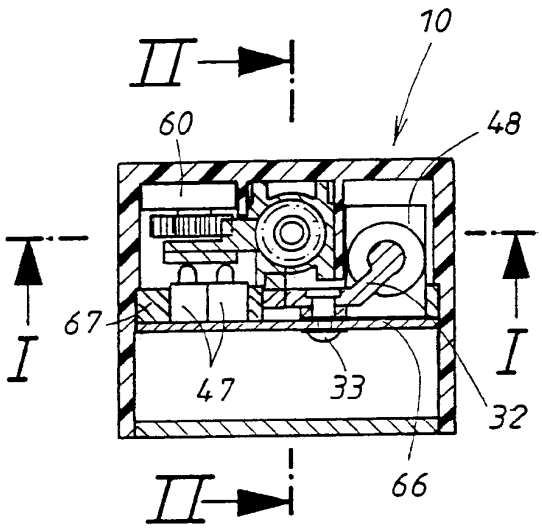


FIG. 3

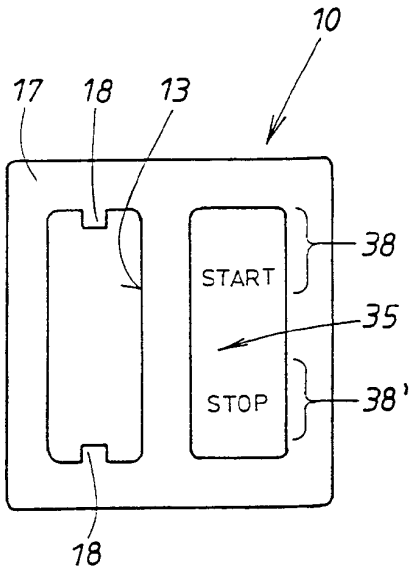


FIG. 4

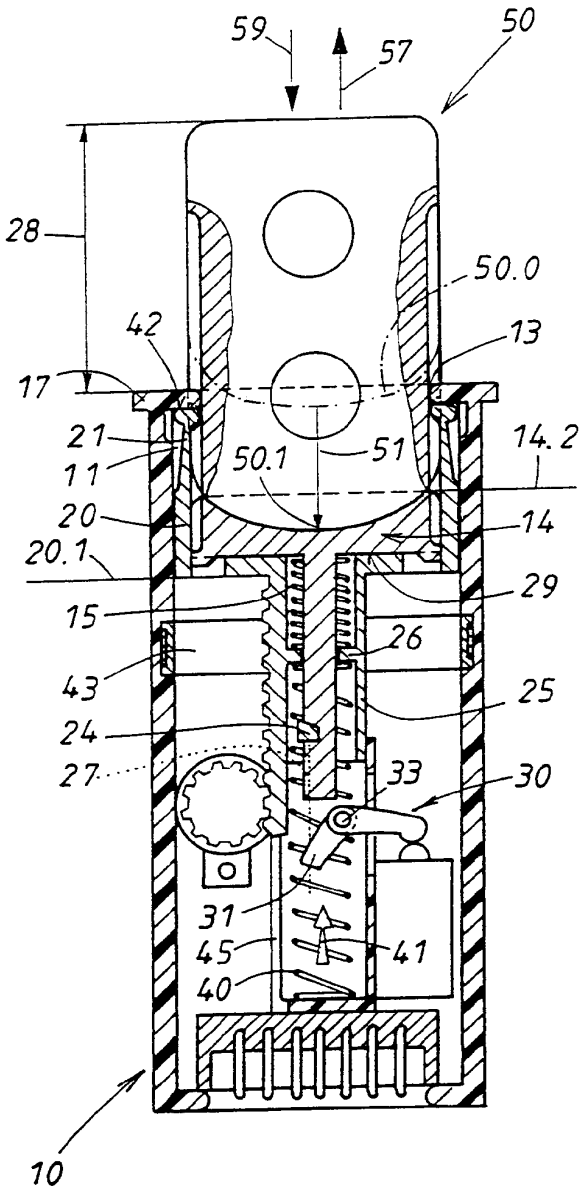

59
57
50
28
50.0
42
13
17
21
11
50.1
51
14.2
20
14
20.1
29
15
26
43
25
24
27
33
30
31
45
41
40
10

FIG. 5

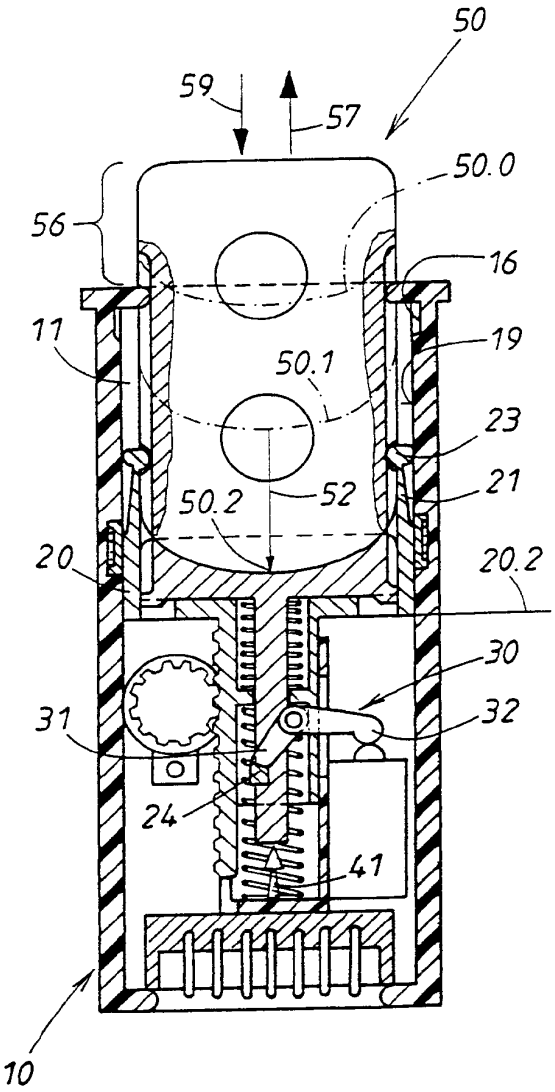

50
59
57
50.0
56
16
11
19
50.1
23
21
50.2
52
20
20.2
30
31
32
24
41
10

FIG. 6

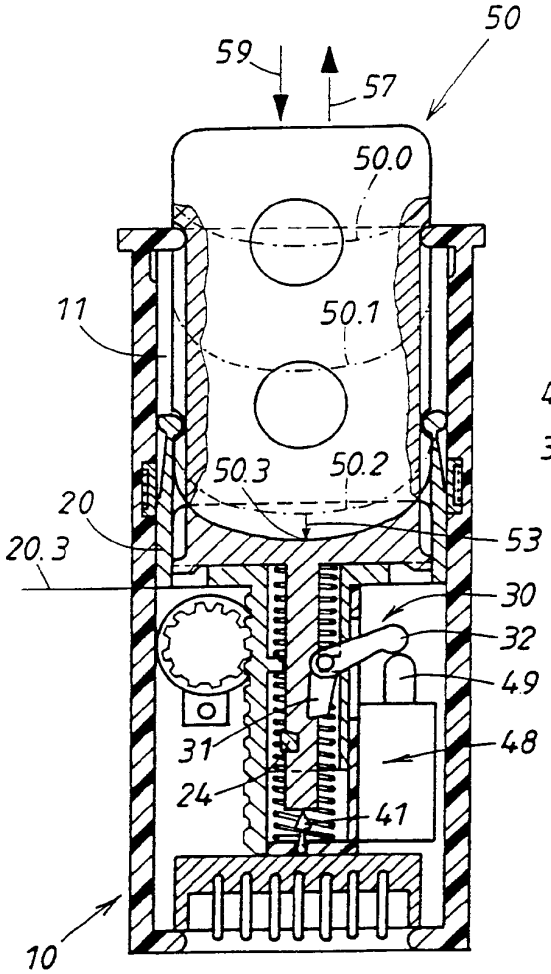

50
59
57
50.0
11
50.1
50.3
50.2
20
20.3
53
30
32
49
48
31
24
41
10

FIG. 7

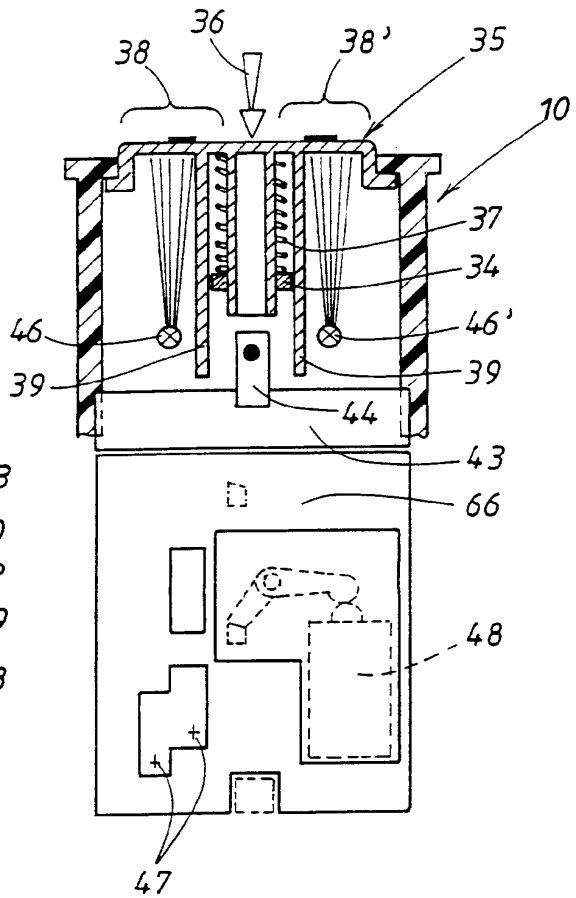

36
38
38'
35
10
37
34
46
46'
39
39
44
43
66
48
47

FIG. 8

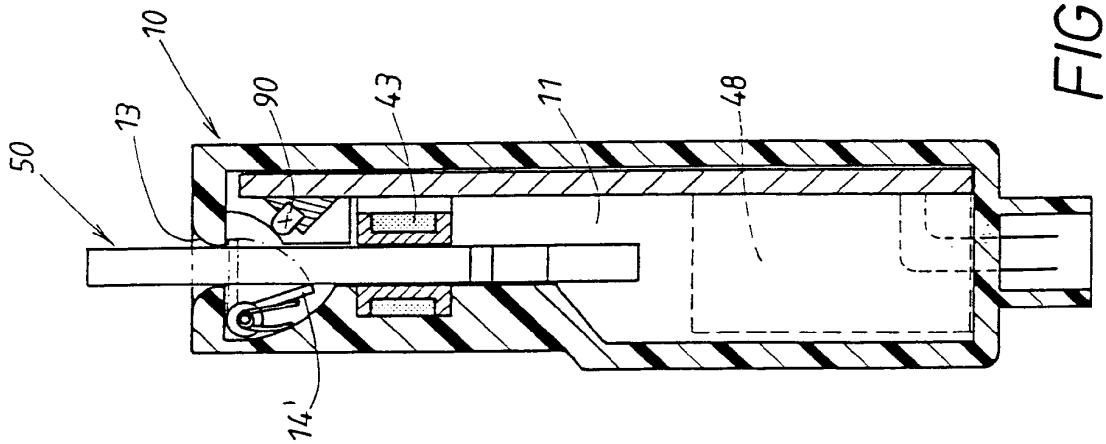

10
13
90
43
11
48
50
14'

FIG. 10

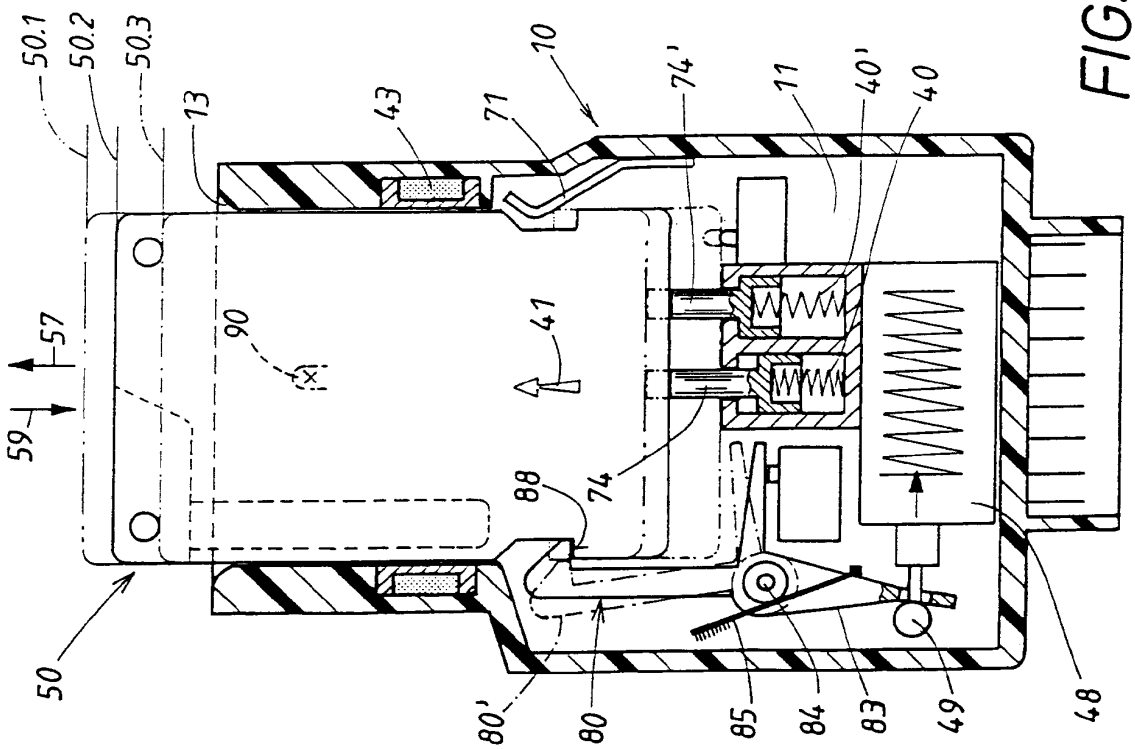

50.1
50.2
50.3
13
43
71
10
74'
11
40'
40
57
59
90
41
88
74
50
80'
80
85
84
83
49
48

FIG. 9

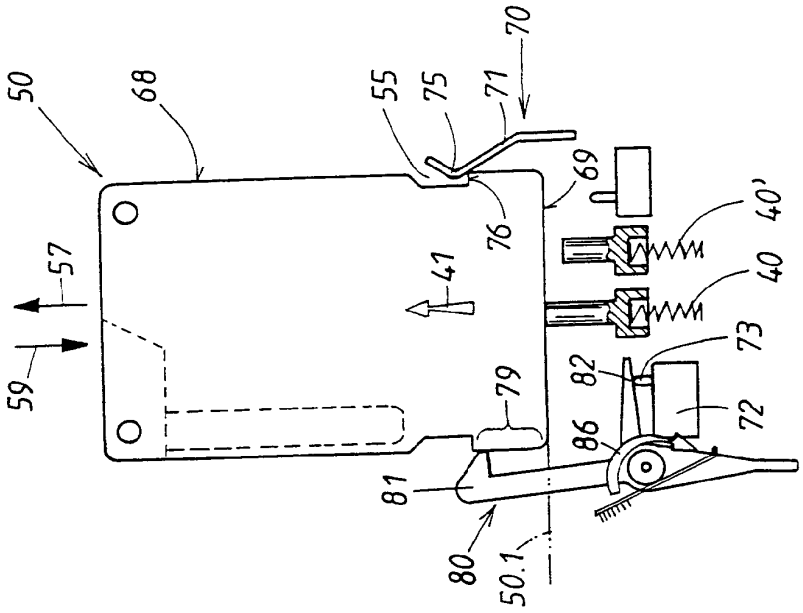

50
68
55
75
71
70
69
40'
40
73
72
82
86
79
81
80
50.1
57
59
41
76

FIG. 12

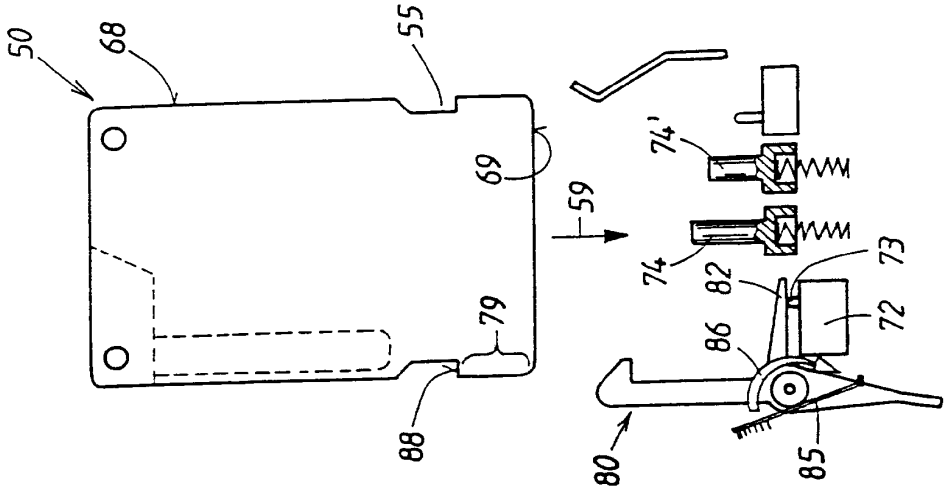

50
68
55
69
59
74'
74
82
73
72
86
79
88
80
85

FIG. 11

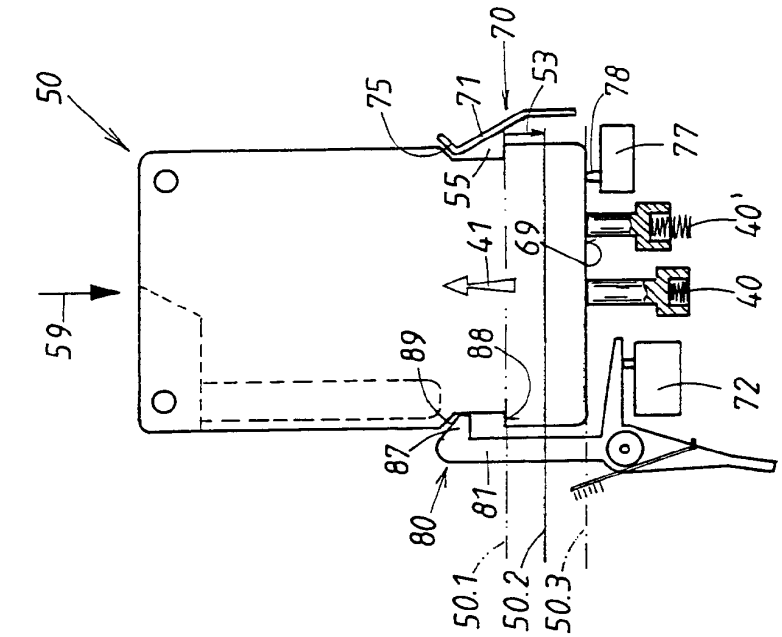


FIG. 14

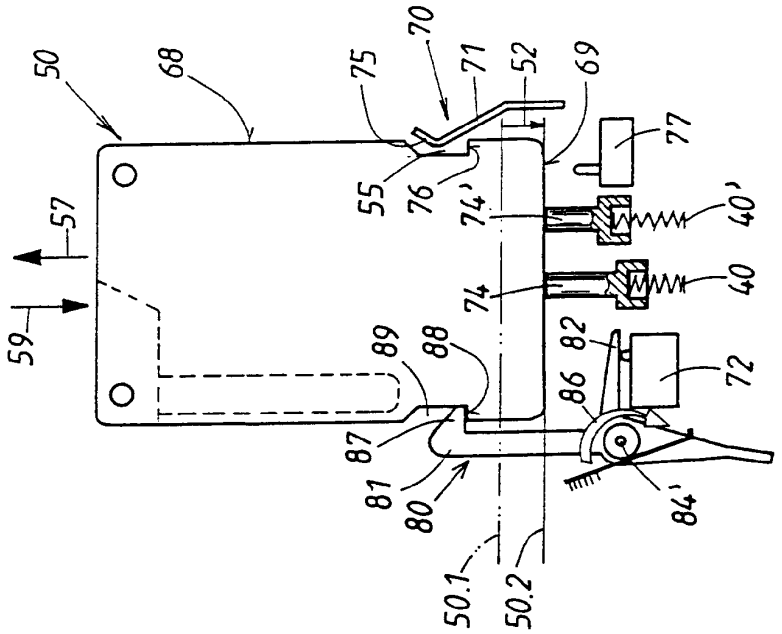


FIG. 13

IPR2022-00412
Apple EX1053 Page 545

INTERNATIONAL SEARCH REPORT

Interr.. ›nal Application No
PCT/EP 00/07769

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 B60R25/04

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 B60R

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DE 33 06 863 A (DAIMLER BENZ AG) 6 September 1984 (1984-09-06)	1-4,28
Y	page 12, paragraph 2 -page 15, paragraph 2	10-12
A	figures 3-8	17
Y	DE 196 41 898 C (KOSTAL LEOPOLD GMBH & CO KG) 13 November 1997 (1997-11-13) column 2, line 30 - line 49; figures 1,2	10,12
Y	DE 197 47 732 A (BOSCH GMBH ROBERT) 20 May 1999 (1999-05-20) column 2, line 6 - line 14	11
A	US 5 254 996 A (CLAAR KLAUS ET AL) 19 October 1993 (1993-10-19) column 5, line 25 -column 6, line 32; figures 1,2	11

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 November 2000	04/12/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Areal Calama, A-A

1

Form PCT/ISA/210 (second sheet) (July 1992)

IPR2022-00412
Apple EX1053 Page 546

INTERNATIONAL SEARCH REPORT

Interr. nal Application No
PCT/EP 00/07769

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
P,X	WO 00 29267 A (BOSCH GMBH ROBERT ;FEUCHTER UWE (DE); GEIL ANDREAS (DE)) 25 May 2000 (2000-05-25) page 14, paragraph 4 -page 18, last paragraph; figures 1-3	1,3,10, 11

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

IPR2022-00412
Apple EX1053 Page 547

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter. nal Application No
PCT/EP 00/07769

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 3306863 A	06-09-1984	NONE	
DE 19641898 C	13-11-1997	NONE	
DE 19747732 A	20-05-1999	AU 1142699 A	17-05-1999
		WO 9921741 A	06-05-1999
US 5254996 A	19-10-1993	DE 4038038 C	02-01-1992
		EP 0492061 A	01-07-1992
		ES 2061141 T	01-12-1994
		JP 2053015 C	10-05-1996
		JP 4273794 A	29-09-1992
		JP 7044729 B	15-05-1995
WO 0029267 A	25-05-2000	DE 19853075 A	25-05-2000

IPR2022-00412
Apple EX1053 Page 548

INTERNATIONALER RECHERCHENBERICHT

Interr. nales Aktenzeichen
PCT/EP 00/07769

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 B60R25/04

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 B60R

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X Y A	DE 33 06 863 A (DAIMLER BENZ AG) 6. September 1984 (1984-09-06) Seite 12, Absatz 2 -Seite 15, Absatz 2 Abbildungen 3-8	1-4,28 10-12 17
Y	DE 196 41 898 C (KOSTAL LEOPOLD GMBH & CO KG) 13. November 1997 (1997-11-13) Spalte 2, Zeile 30 - Zeile 49; Abbildungen 1,2	10,12
Y	DE 197 47 732 A (BOSCH GMBH ROBERT) 20. Mai 1999 (1999-05-20) Spalte 2, Zeile 6 - Zeile 14	11
A	US 5 254 996 A (CLAAR KLAUS ET AL) 19. Oktober 1993 (1993-10-19) Spalte 5, Zeile 25 -Spalte 6, Zeile 32; Abbildungen 1,2	11

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
28. November 2000	04/12/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Areal Calama, A-A

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

IPR2022-00412
Apple EX1053 Page 549

INTERNATIONALER RECHERCHENBERICHT

Interi. ,nales Aktenzeichen
PCT/EP 00/07769

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
P,X	WO 00 29267 A (BOSCH GMBH ROBERT ;FEUCHTER UWE (DE); GEIL ANDREAS (DE)) 25. Mai 2000 (2000-05-25) Seite 14, Absatz 4 -Seite 18, letzter Absatz; Abbildungen 1-3	1,3,10, 11

1

Formblatt PCT/ISA/210 (Fortsetzung von Blatt 2) (Juli 1992)

IPR2022-00412
Apple EX1053 Page 550

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Interna...ales Aktenzeichen
PCT/EP 00/07769

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 3306863 A	06-09-1984	KEINE	
DE 19641898 C	13-11-1997	KEINE	
DE 19747732 A	20-05-1999	AU 1142699 A	17-05-1999
		WO 9921741 A	06-05-1999
US 5254996 A	19-10-1993	DE 4038038 C	02-01-1992
		EP 0492061 A	01-07-1992
		ES 2061141 T	01-12-1994
		JP 2053015 C	10-05-1996
		JP 4273794 A	29-09-1992
		JP 7044729 B	15-05-1995
WO 0029267 A	25-05-2000	DE 19853075 A	25-05-2000

IPR2022-00412
Apple EX1053 Page 551

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
31. Mai 2001 (31.05.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/38673 A1

(51) Internationale Patentklassifikation[7]: E05B 19/04, A45C 11/32

(21) Internationales Aktenzeichen: PCT/EP00/11504

(22) Internationales Anmeldedatum:
18. November 2000 (18.11.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 56 392.6 24. November 1999 (24.11.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **HUF HÜLSBECK & FÜRST GMBH & CO. KG** [DE/DE]; Steeger Strasse 17, 42551 Velbert (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **WITTWER, Reinhard** [DE/DE]; Beuthener Strasse 26, 42579 Heiligenhaus (DE). **BARRENBERG, Günter** [DE/DE]; Am Buschkothen 20, 42551 Velbert (DE). **HABECKE, Mathias** [DE/DE]; Nikolaus-Gross-Strasse 12, 45529 Hattingen (DE). **JACOB, Dirk** [DE/DE]; Breslauer Strasse 13, 42579 Heiligenhaus (DE).

(74) Anwalt: **MENTZEL, Norbert**; Kleiner Werth 34, 42275 Wuppertal (DE).

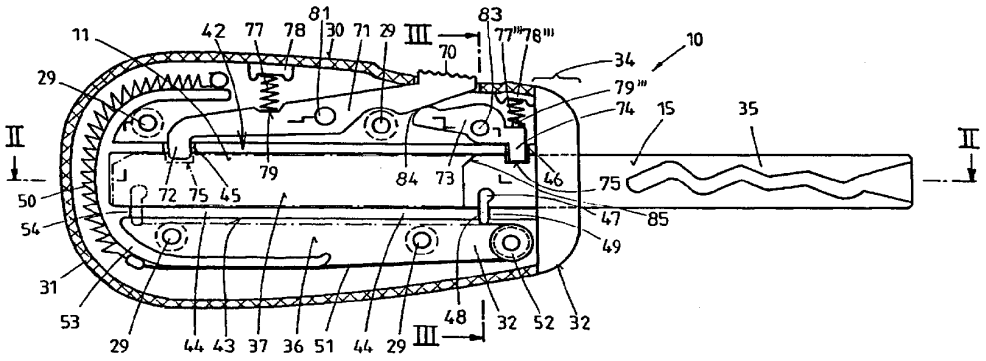
(81) Bestimmungsstaaten *(national)*: AU, BR, CN, IN, JP, KR, US.

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

[Fortsetzung auf der nächsten Seite]

(54) Title: KEY, IN PARTICULAR FOR A MOTOR VEHICLE

(54) Bezeichnung: SCHLÜSSEL, INSBESONDERE FÜR KFZ



(57) **Abstract:** The invention relates to a key, in particular for a motor vehicle, comprising a housing (30) and a mechanical key part (35) connected thereto. In keys of this type, the locking element of the key part is usually converted from an inoperative position (11) into a working position (15), in which the key (10) can be used to mechanically operate a lock or a locking cylinder, by means of a mechanism (47, 50, 51, 52, 60, 61, 62, 64, 65, 66) which is located in the housing. In order to improve a key of this type, the invention proposes the provision of a traction or force of pressure regulator (50) for the mechanism (47, 50, 51, 52, 60, 61, 62, 64, 65, 66) which acts indirectly upon the actuator (47) via traction or thrust means (51).

(57) **Zusammenfassung:** Die Erfindung betrifft einen Schlüssel, insbesondere für Kfz mit einem Gehäuseteil (30) und einem daran angeordneten mechanischen Schlüsselteil (35). Bei solchen Schlüsseln ist es bekannt, den schliesswirksamen Teil des Schlüsselteils mittels einer Mimik (47, 50, 51, 52, 60, 61, 62, 64, 65, 66), welche im Gehäuse angeordnet ist, von einer Ruhestellung (11) in eine Arbeitsstellung (15) zu überführen, in der der Schlüssel (10) zur mechanischen Betätigung eines Schlosses oder Schliesszylinders benutzt werden kann. Zur Verbesserung eines derartigen Schlüssels wird vorgeschlagen, dass die Mimik (47, 50, 51, 52, 60, 61, 62, 64, 65, 66) einen Zug- (50) oder Druckkraftspeicher umfasst, der indirekt über ein Zug- (51) oder Schubmittel an dem Stellglied (47) angreift.

WO 01/38673 A1

IPR2022-00412
Apple EX1053 Page 552

Veröffentlicht:
— *Mit internationalem Recherchenbericht.*
— *Vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen.*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Schlüssel, insbesondere für Kfz

Die Erfindung richtet sich auf einen Schlüssel der in Anspruch 1 genannten Art. Derartige Schlüssel kommen insbesondere bei Kraftfahrzeugen zur Anwendung.

Aus der US 2,690,666, als nächstliegenden Stand der Technik, ist ein Schlüsselhalter bekannt, bei dem in einem Gehäuse befindliche Schlüssel über ihnen zugeordnete Druckfedern aus dem Gehäuse herausbewegt werden können. Bei diesem Schlüsselhalter kann jeweils ein Schlüssel über einen Wahlschalter ausgewählt werden, und der Schlüssel dann durch Betätigung eines Auslösemittels freigegeben werden. Der ausgewählte Schlüssel wird daraufhin von der Kraft der Druckfeder aus dem Gehäuse heraus in seine Arbeitsstellung überführt. Die Federn greifen bei dem Gegenstand der US-Schrift direkt am hinteren Ende der Schlüssel an, so daß sie in der Ruhestellung des Schlüssels im Gehäuseinnenraum einen erheblichen Teil der Baulänge des Schlüsselgehäuses einnehmen. Eine erhöhte Baulänge ist jedoch insbesondere bei Kfz-Schlüsseln nicht wünschenswert, die während des Betriebes eines Kfz in dessen Zündschloß verbleiben, da durch die in

IPR2022-00412
Apple EX1053 Page 554

den Bewegungsraum eines Knies hineinragenden Schlüssel das Verletzungsrisiko im Bereich des rechten Knies einer Fahrerin oder eines Fahrers erhöht wird.

Aus der US 2,550,375 ist ebenfalls ein in einem Gehäuse lateral verschieblich angeordneter Schlüssel bekannt. Auch bei diesem Schlüssel ist im rückwärtigen Bauraum des Schlüssels ein Federglied angeordnet, welches direkt auf den Schlüssel einwirkt. Das Federglied ist hier jedoch als Zugfeder ausgeführt, welches den Schlüssel von seiner ausgeschobenen Lage in seine eingezogene Position automatisch zurückfährt, wenn eine Auslösetaste betätigt wird, die den Schlüssel freigibt.

Aus der DE-GM 17 13 197 ist ein Schlüsselgehäuse bekannt, bei dem ein darin liegender Schlüssel über eine manuelle Betätigung aus dem Gehäuse heraus oder in das Gehäuse hineingeschoben werden kann. Die Betätigung des Schlüssels über eine auf diesen einwirkende Mimik ist dieser Schrift nicht zu entnehmen. Der in dem Gehäuse befindliche Schlüssel kann lediglich über ein oder mehrere Federelemente in seiner im Gehäuse eingezogenen oder aus dem Gehäuse herausgeschobenen Stellung fixiert werden.

Bei einem von der Firma Huf gefertigten Elektronischen-Mechanischen-Schlüssel ist es bekannt, einen mechanischen Schlüsselteil aus- und einklappbar an einem Schlüsselgehäuse anzuordnen. Bei diesem Schlüssel ist die Schlüsselelektronik in einem ersten Gehäuseteil und der mechanische Schlüsselteil in und an einem zweiten Gehäuseteil angeordnet. Die Schnittstellen zwischen dem ersten und dem zweiten Gehäuseteil sind bei diesem Schlüssel sehr verwinkelt und maßlich kompliziert.

Der mechanische Schlüsselteil liegt im eingeklappten Zustand an einer Längsseite des Schlüsselgehäuses, innerhalb einer Eintiefung, die als Schlüsselaufnahme dient.

Der Schlüssel ist in der Aufnahme des Gehäuses an seiner in Ausklapprichtung liegenden Seite offen zugänglich.

Außen an dem Schlüssel ist eine Auslösetaste angeordnet, über deren Betätigung der Schlüssel von seiner Ruhestellung am Gehäuse in eine Arbeitsstellung ausgeklappt werden kann, in der das mechanische Schlüsselteil z.B. zur Betätigung eines Schließzylinders oder eines Zündschlosses benutzt werden kann. Der Ausklappvorgang geschieht nach Betätigen der Auslösetaste automatisch über einen im Schlüsselgehäuse angeordneten Federtrieb der auf den mechanischen Schlüsselteil wirkt.

Zum Einklappen des mechanischen Schlüsselteils muss erneut die Auslösetaste gedrückt werden und der Schlüssel dann manuell wieder in seine Ruhestellung in der seitlich am Gehäuse angeordneten Aufnahme eingeklappt werden.

Von Nachteil bei einem derartigen Schlüssel ist es, dass sich an dem in der Aufnahme offen zugänglichen Schlüssel Dreckpartikel sammeln, die über den mechanischen Schlüsselteil in den zu betätigenden Schließzylinder und/oder des Zündschloss etc. gelangen und diese dadurch auf Dauer verschmutzen und gegebenenfalls funktionsuntüchtig werden können. Auch ist die Öffnung in die der Schlüssel einklappen kann optisch unschön.

Aus der DE 296 18 616 U1 ist ein Kraftfahrzeugschlüssel bekannt, der ebenfalls über eine Mimik von einer an einer Gehäuseseite angeklappten Lage in eine aus dem Gehäuse herausstehende, ausgeklappte Arbeitslage überführbar ist.

Aufgabe der vorliegenden Erfindung ist es, einen Schlüssel bereitzustellen, der einen verhältnismäßig kurzen Bauraum aufweist und der ein gutes optisches Erscheinungsbild aufweist.

Dieses wird erfindungsgemäß durch die im Anspruch 1 genannten Maßnahmen erreicht, denen folgende besondere Bedeutung zukommt. Zur Lösung der patentgemäßen Aufgabe wird vorgeschlagen, das Schlüsselteil in seiner Ruhestellung innen im Gehäuse anzuordnen, wobei das Schlüsselteil nach Betätigung der Auslösetaste über eine in dem Gehäuse angeordnete Mimik von seiner Ruhestellung im Inneren des Gehäuses durch eine Längsverschiebung in seine Arbeitsstellung überführt wird, in der zumindest der schließwirksame Teil des mechanischen Schlüsselteils außerhalb des Gehäuses liegt. Hierzu weist die Mimik einen Zug- oder Druckkraftspeicher auf, der indirekt über ein Zug- oder Schubmittel an dem Stellglied des Schlüsselteils angreift. Durch diese Maßnahmen ist es nicht mehr notwendig, den Zug- oder Druckkraftspeicher in unmittelbarer Nachbarschaft zum mechanischen Schlüsselteil anzuordnen, um das Bewegungsmoment vom Zuf- oder Druckkraftspeicher auf das mechanische Schlüsselteil zu übertragen. Vielmehr wird es möglich, den Zug- oder Druckkraftspeicher an jeder beliebigen Position im Schlüsselgehäuse anzuordnen. So kann der Zug- oder Druckkraftspeicher insbesondere auch seitlich, neben dem im Gehäuse eingezogenen Schlüssel angeordnet werden. Der Bauraum, insbesondere die Bauraumlänge des Schlüsselgehäuses kann hierdurch vermindert werden. Ebenfalls wird eine größere Variationsbreite bei der Formgestaltung des Schlüsselgehäuses ermöglicht. Der Zugkraftspeicher könnte z.B. eine zugbelastete Feder, ein Gummielement, eine Unterdruckkammer, ein Solenoid etc. sein. Als Druckkraftspeicher können z.B. vorgesehen sein linear wirkende Druckfedern, Spiralfedern, elastische Elemente (z.B. aus Kunststoff), Druckkörper, Solenoide etc.

Bei der indirekten Übertragung der Verstellbewegung vom Druckkraftspeicher auf das mechanische Schlüsselteil kann das Schubmittel z.B. ein Treibriemen, eine Stellkette, ein Stellband, ein Zahnriemen, ein Zahnrad etc. sein.

IPR2022-00412
Apple EX1053 Page 557

Um ein reibungsloses Herausfahren des mechanischen Schlüsselteils zu gewährleisten, sind im Innenraum des Gehäuses Mittel angeordnet, durch die das Schlüsselteil bei der Längsbewegung von seiner Ruhestellung in seine Arbeitsstellung geführt ist.

Ein weiterer Vorteil der sich aus der erfindungsgemäßen Lösung gemäß Anspruch 1 ergibt ist der, dass an dem Schlüsselgehäuse nunmehr glatte Flächen überwiegen und keine vorstehenden Kanten und unschöne Vertiefungen mehr vorhanden sind, so dass der Schlüssel eine sehr ansprechende Optik aufweist.

Außerdem ist die Bedienungsfreundlichkeit durch das automatische Ausfahren des mechanischen Schlüsselteils und dem einfach zu bewirkenden Wiedereinschieben desselben verbessert worden.

Vorteilhaft nach Anspruch 2 kann es auch sein, wenn die Schlüsselöffnung im Gehäuseteil im wesentlichen formschlüssig zur Außenkontur des mechanischen Schlüsselteils ausgeführt ist, so dass möglichst wenig Öffnungsraum zwischen Gehäusewand und Schlüsselteil vorhanden ist, an dem Schmutzpartikel in das Gehäuseinnere eindringen können. Ferner wird durch die formschlüssige Ausführung der Öffnung ein Abstreifen von eventuell während oder nach der Betätigung aufgefangenen Schmutzpartikeln ermöglicht.

In einer weiteren günstigen Ausführungsform der Erfindung kann gemäß Anspruch 3 auch ein Mittel zum Verschließen der Schlüsselöffnung, wie etwa eine Klappe oder ein Schieber, der manuell oder automatisch betätigt wird, vorgesehen sein, der das Gehäuseteil in der Ruhestellung des darin angeordneten mechanischen Schlüsselteils gegen ein Eindringen von Schmutz gänzlich abriegelt.

Vorteilhaft gemäß Anspruch 4 kann es sein, wenn das Schlüsselteil innerhalb des Gehäuseteils in einem Führungskanal liegt, innerhalb dessen das Schlüsselteil bei

IPR2022-00412
Apple EX1053 Page 558

seiner Längsverschiebung geführt ist. Günstigerweise können zur Erzeugung des Führungskanals auch umgebende Gehäusewände wie z.B. die an den Flächenseiten des umgebenden Gehäuseteils liegenden Wände zur Ausbildung des Führungskanals herangezogen werden.

Der Führungskanal kann eine seitliche Öffnung aufweisen, durch den ein Stellglied, wie etwa ein Zahnrad oder ein Mitnehmerzapfen, auf das mechanische Schlüsselteil einwirken kann und derart eine von der Mimik ausgeübte Verstellbewegung auf das mechanische Schlüsselteil überträgt.

Günstig kann es auch sein, wenn Rastmittel vorgesehen sind, die das mechanische Schlüsselteil in seiner Ruhe- und in seine Arbeitsstellung im wesentlichen bewegungsstarr halten. Nach Betätigung der Auslösetaste oder eines anderen Auslösemittels geben die Rastmittel das mechanische Schließteil frei, so dass diese von der einen Stellung in die andere Stellung verfahrbar ist. Die Rastmittel können z.B. an einem oder mehreren Hebeln angeordnete Haken umfassen, die in der Raststellung in eine am Umfang des Schließteils befindliche Aussparung eingreifen, oder die in einem Vorsprung, einer Nase, einem Gegenrastglied etc. eines zur Mimik gehörenden Stellmittels angreifen und derart indirekt das mechanische Schließteil in seiner Arbeits- oder Ruhestellung halten.

Bei der Verwendung eines Zugkraftspeichers kann es günstig sein, wenn der Zugweg des Zugkraftspeichers und/oder des durch den Zugkraftspeichers betätigten Zugmittels durch ein- oder mehrfache Umlenkung des Zugkraftspeichers und/oder des Zugmittels an einem oder mehreren Umlenkteilen, wie z.B. Umlenkrollen oder Umlenkstegen vergrößert ist. Durch diese Maßnahme wird ein weitgehendes Herausfahren des mechanischen Schließteils bei der Überführung von seiner Ruhestellung in seine Arbeitsstellung erreicht.

IPR2022-00412
Apple EX1053 Page 559

Es kann ferner vorteilhaft sein, die Schlüsselelektronik und die Schlüsselmechanik in zwei, in sich abgeschlossenen Gehäuseteilen anzuordnen, die beide entlang ebener Verbindungsflächen lösbar aneinander festgelegt sind. Günstigerweise ist der Batteriedeckel derart an dem Gehäuseteil angeordnet das die Schlüsselelektronik aufweist, dass er durch das gegenüberliegende Gehäuseteil mit der Mechanik darin verdeckt wird. Zum Wechseln der Batterie muss also lediglich eine Trennung der beiden Gehäuseteile voneinander vorgenommen werden um danach den Batteriedeckel öffnen zu können. Zur Verbindung der beiden Gehäuseteile sind die verschiedensten Verbindungsmittel denkbar. So können z.B. Schwalbenschwanznuten oder -vertiefungen und Schwalbenschwanzvorsprünge - oder -erhöhungen an den Gehäuseteilen angeordnet sein, die ineinandergeschoben die Verbindung der beiden Gehäuseteile gewährleisten.

Weitere Vorteile und Maßnahmen der Erfindung ergeben sich aus den Unteransprüchen, der nachfolgenden Beschreibung und den Zeichnungen. In den Zeichnungen ist die Erfindung in drei Ausführungsbeispielen dargestellt. Es zeigen:

Fig. 1 schematisch eine erste Ausführungsform eines erfindungsgemäßen Schlüssels im Schnitt durch das zweite, die Mechanik enthaltene Gehäuseteil,

Fig. 2 schematisch, die erste Ausführungsform eines erfindungsgemäßen Schlüssels im Schnitt gemäß II - II aus Fig. 1,

Fig. 3 schematisch, die erste Ausführungsform des erfindungsgemäßen Schlüssels im Schnitt gemäß III - III aus Fig. 1,

IPR2022-00412
Apple EX1053 Page 560

Fig. 4 schematisch, das erste Gehäuseteil der ersten Ausführungsform des erfindungsgemäßen Schlüssels mit der Schlüsselelektronik gemäß dem Schnitt IV - IV aus Fig. 2,

Fig. 5 schematisch, das zweite Gehäuseteil der ersten Ausführungsform des erfindungsgemäßen Schlüssels mit dem mechanischen Schlüssel im Schnitt gemäß V - V aus Fig. 2,

Fig. 6 schematisch, die erste Ausführungsform des erfindungsgemäßen Schlüssels in Seitenansicht, bei dem beide Gehäuseteile aneinander festgelegt sind,

Fig. 7 schematisch, die erste Ausführungsform des erfindungsgemäßen Schlüssels, bei dem die Verbindungsmittel der beiden Gehäuseteile gelöst sind,

Fig. 8 schematisch, die erste Ausführungsform des erfindungsgemäßen Schlüssels in einem Schnitt entlang VIII - VIII aus Fig. 6,

Fig. 9 schematisch, ein zweites Ausführungsbeispiel eines erfindungsgemäßen Schlüssels, in einem Schnitt durch das zweite Gehäuseteil mit der Schlüsselmechanik,

Fig. 10 schematisch, die zweite Ausführungsform des erfindungsgemäßen Schlüssels im Schnitt gemäß X - X aus Fig. 9,

Fig. 11 schematisch, eine dritte Ausführungsform des erfindungsgemäßen Schlüssels im Schnitt durch das die

IPR2022-00412
Apple EX1053 Page 561

Mechanik aufweisende zweite Gehäuseteil, in der Ruhestellung des mechanischen Schlüsselteils,

Fig. 12 schematisch, die dritte Ausführungsform des erfindungsgemäßen Schlüssels gemäß Fig. 11 in der Arbeitsstellung des mechanischen Schlüsselteils.

In den Fig. 1 bis 8 ist eine erste Ausführungsform des erfindungsgemäßen Schlüssels 10 dargestellt. Bei dieser Ausführungsform setzt sich der Schlüssel zusammen aus einem ersten Gehäuseteil 20 und einem zweiten Gehäuseteil 30. Das erste Gehäuseteil umfasst eine Gehäusegrundplatte 22 und einen Gehäusedeckel 21. In dem Gehäusedeckel 21 sind Tastfelder 26 angeordnet, über die eine im Inneren des ersten Gehäuseteiles 20 liegende Elektronik 25 betätigt werden kann. In der Gehäusegrundplatte 22 ist ein Batteriefachdeckel 23 angeordnet, über den eine Batterie 24, die der Stromversorgung der Elektronik 25 dient, in das Gehäuseteil 20 ein- und ausgeführt werden kann. Das erste Gehäuseteil 20 ist wasserdicht verschlossen, wobei der Gehäusedeckel 21 an der Gehäusegrundplatte 22 über Schraubmittel 29 festgelegt ist. An dem Schlüssel 10 ist in diesem Ausführungsbeispiel noch eine Öse 19 vorgesehen, an die z.B. ein Schlüsselanhänger angebracht werden kann.

An dem ersten Gehäuseteil 20 ist entlang einer planaren Ebene 14 ein zweites Gehäuseteil 30 angeordnet. Das zweite Gehäuseteil 30 besteht in diesem Ausführungsbeispiel ebenfalls aus einer Gehäusegrundplatte 32 und einem diese abdeckenden Gehäusedeckel 31. Beide Gehäuseteile 20 und 30 sind über Verbindungsmittel 28, 33 lösbar miteinander verbunden. Bei diesen Verbindungsmitteln handelt es sich in diesem Ausführungsbeispiel um Verrastmittelvorsprünge 28, die in Nuten 27 in der Gehäusegrundplatte 32 des ersten Gehäuseteiles 20 angeordnet sind und auf Seiten des zweiten Gehäuseteiles 30 um Schwalbenschwanzzapfen 33, die an der Gehäusegrundplatte 32 angeformt

IPR2022-00412
Apple EX1053 Page 562

sind. Um beide Gehäuseteile 20, 30 voneinander zu lösen, z.B. zum Zwecke des Austausches der Batterie 23, werden beide Gehäuseteile in Demontagerichtung 17 (Fig. 7) gegeneinander verschoben, wobei ein Anfangswiderstand zu überwinden sein kann. Die Schwalbenschwanzzapfen 33 befinden sich nach dieser Verschiebung gemäß Pfeil 17 in dem offenen Teil der Nut 27, so dass nun beide Gehäuseteile 20, 30 voneinander getrennt werden können. Zur Montage müssen die beiden Gehäuseteile 20 und 30 in entsprechender Weise aneinandergesetzt werden, wobei die Schwalbenschwanzzapfen 33 in die Nut 27 an dem gegenüberliegenden Gehäuseteil eingeführt werden müssen, und das Gehäuseteil 20 daraufhin in Montagerichtung 18 (Fig. 7) gegenüber dem Gehäuseteil 30 verschoben werden. Die Schwalbenschwanzzapfen 33 verhaken sich dabei hinter dem Verrastmittelvorsprung 28 in der Gehäusegrundplatte 22 des ersten Gehäuseteiles, wodurch beide Gehäuseteile 20, 30 aneinander festgelegt werden. Durch das Festlegen der beiden Gehäuseteile entlang einer Ebene wird die vorbeschriebene Montage/Demontage vereinfacht.

In dem zweiten Gehäuseteil 30 ist eine Schlüsselmechanik angeordnet, über die ein mechanisches Schlüsselteil 35, welches sich in einer Ruhestellung 11 im Gehäuseinnenraum 36 des zweiten Gehäuseteils 30 befindet, durch Betätigung eines Auslösemittels, wie etwa einer Auslösetaste 70 automatisch in eine Arbeitsstellung 15 verfahren werden kann, in der das mechanische Schlüsselteil 35 zur Betätigung eines Schließzylinders oder eines Zündschlosses etc. verwendet werden kann. Das mechanische Schlüsselteil 35 ist dazu in dem vorliegenden Ausführungsbeispiel gemäß den Fig. 1 bis 8 wie folgt in dem zweiten Gehäuseteil 30 angeordnet.

Im Gehäuseinnenraum 36 des zweiten Gehäuseteils 30 ist ein Führungskanal 37 angeordnet, dessen beide Flächenwände 40 und 41 aus den Flächenseiten 38 und 39 der angrenzenden Gehäusegrundplatte 32 und des Gehäusedeckels 31 gebildet wird. Der Führungskanal 37 wird weiterhin zu seinen beiden Seiten von den Wänden 42 und 43 begrenzt. In dem Führungskanal 37 ist das mechanische Schlüsselteil 35

IPR2022-00412
Apple EX1053 Page 563

verschiebbar angeordnet. Dieser Führungskanal 37 ist an seinem vorderen Ende mit einer Schlüsselöffnung 12 versehen, durch die das mechanische Schlüsselteil 35 aus dem Gehäuseteil 20 heraus in seiner Arbeitsstellung 15 gelangen kann. In seinem hinteren Bereich ist der Führungskanal 37 in diesem Ausführungsbeispiel durch eine Führungswand 53 abgeschlossen. An der, der Wand 42 zugewandten Schmalseite des mechanischen Schlüsselteils 35 ist eine Aussparung 75 im hinteren Bereich des mechanischen Schlüsselteils 35 angeordnet. In dieser Aussparung 75 greift in der Ruhestellung 11 der Rasthaken 72 eines Hebels 71, durch den das mechanische Schlüsselteil 35 in der Ruhestellung 11 gehalten wird. Der Rasthaken 72 wird dabei mit der Kraft eines Druckmittels 77, wie etwa einer Feder, die an der Ansatzstelle 79 am Hebel 71 angreift und die anderenends in einem Federsitz 78 an der Wand des Gehäusedeckels 31 abgestützt ist, in der Aussparung 75 gehalten. Der Hebel 71 ist an einer Achse 81 schwenkbar gelagert. Der Hebel 71 ist über eine Auslösetaste 70, die in diesem Ausführungsbeispiel an den Hebel 71 angeformt ist, zu betätigen, wodurch der Rasthaken 72 aus der Aussparung 75 ausrastet, wenn das mechanische Schlüsselteil 35 in seiner Ruhestellung 11 sitzt.

Damit der Rasthaken 72 die Wand 42 durchgreifen kann, um in die Aussparung 75 im mechanischen Schlüsselteil 35 einzugreifen, ist in der Wand 42 eine Öffnung 45 vorgesehen.

Im vorderen Bereich des Schlüssels 10 unmittelbar hinter einem Frontteil 34 der Gehäusegrundplatte, in welcher die Schlüsselöffnung 12 sitzt, ist ein zweiter Hebel 73 angeordnet, der um eine Achse 83 verschwenkbar ist, und der einen Rasthaken 74 aufweist, der in der Arbeitsstellung 15 des mechanischen Schlüsselteils 35 in die Aussparung 75 im mechanischen Schlüsselteil 35 eingreift. In der Wand 42 des Führungskanals 37 ist wiederum eine Öffnung 46 vorgesehen, die ein Durchgreifen der Wand 42 durch den Rasthaken 74 erlaubt. Der Rasthaken 74 wird wiederum mittels der Kraft einer Feder 79‘‘‘, die an den Ansatzstellen 77‘‘‘ und 78‘‘‘ zwischen dem Hebel 73 und der Wand 42 des Gehäuseteils 31 festgelegt ist. Der

IPR2022-00412
Apple EX1053 Page 564

Hebel 73 steht an der Berührungsstelle 84 in mechanischem Kontakt mit dem Hebel 71. Bei einer Betätigung der Auslösetaste 70 wird hierdurch, neben dem Hebel 71, auch der Hebel 73 betätigt und der Rasthaken 74 aus dem Führungskanal 37 und gegebenenfalls aus der Aussparung 75 herausgezogen, wenn das mechanische Schlüsselteil 35 in seiner Arbeitsstellung 15 sitzt. Der aus den Hebeln 71 und 73 gebildete Doppelhebel ermöglicht es, dass an dem mechanischen Schlüsselteil nur eine Aussparung 75 am Ende des Schaftes des Schlüsselteils erforderlich ist.

Das mechanische Schlüsselteil 35 kann über eine Mimik nach Betätigung der Auslösetaste 70 automatisch aus seiner Ruhestellung 11 in die Arbeitsstellung 15 überführt werden. Hierzu ist in dem vorliegenden Ausführungsbeispiel zunächst ein Zugkraftspeicher 50 in Form einer Zugfeder vorgesehen, die im hinteren Bereich des Gehäuseteils 30 angeordnet ist. Die Feder 50 ist mit einem Zugmittel 51 wie etwa einem Kunststoffstrang oder Kunststoffband verbunden, wobei die Feder 50 und Zugmittel 51 im hinteren Bereich des Gehäuseteils 30 entlang der Führungswand 53 geführt sind. Das Zugmittel 51 ist andernends wiederum an einem Stellglied 47 festgelegt, welches seinerseits fest verbunden mit dem mechanischen Schlüsselteil 35 ist, welches im hinteren Bereich des Schlüsselteils 35 angeordnet ist. Das Zugmittel 51 ist im vorderen Bereich des Gehäuseteils 30 um eine Umlenkrolle 52 herumgeführt, so dass der Zugweg der Feder 50 und des Zugmittels 51 parallel zur Ausschubrichtung 16 und zum Verlauf des Führungskanals 37 des mechanischen Schlüsselteils 35 verläuft. In der Seitenwand 43 des Führungskanals 37 ist eine längliche Öffnung 44 vorgesehen, durch die das Stellglied 47 hindurchgreift. Das Zugmittel 51 ist auf der dem Führungskanal 37 abgewandten Seite des Stellgliedes 47 mit dessen Nase 48 verbunden.

In der Ruhestellung 11 des mechanischen Schlüsselteils 35 befindet sich die Nase 48 des Stellgliedes 47 an dem, die Längsöffnung 44 im rückwärtigen Bereich begrenzenden Anschlag 54. Der Schlüssel ist in der Ruhestellung 11 gänzlich in das Gehäuseteil 30 eingefahren. Zur Überführung des mechanischen Schlüsselteils 35 in

seiner Arbeitsstellung 15 muss nun die Auslösetaste 70 und somit der Hebel 71 betätigt werden, so dass der Rasthaken 72 aus der Aussparung 75 im mechanischen Schlüsselteil 35 herausfährt. Das mechanische Schlüsselteil 35 verfährt nun unter Einwirkung des Zugkraftspeichers 50 in Ausschubrichtung 16 aus dem Gehäuseteil 30 hinaus in seine Arbeitsstellung 15. Bei Erreichen der Arbeitsstellung 15 fährt die Nase 48 des Stellgliedes 47 gegen den Anschlag 49, der die Öffnung 44 an ihrem der Schlüsselöffnung zugewandten Ende begrenzt. Sobald das mechanische Schlüsselteil 35 in dieser Stellung ist, rastet zusätzlich noch der Rasthaken 74 in der Aussparung 75 am mechanischen Schlüsselteil 35 unter der Kraft der Feder 77‘‘‘ ein.

Zum Rücküberführen des mechanischen Schlüsselteiles 35 aus seiner Arbeitsstellung 15 in die Ruhestellung 11 muss wiederum die Auslösetaste 70 manuell betätigt werden, wodurch der Hebel 73 verschwenkt wird und der daran angeordnete Rasthaken 74 aus der Aussparung 75 im mechanischen Schlüsselteil 35 herausfährt. Hierdurch kann nun das mechanische Schlüsselteil 35 manuell wieder in den Führungskanal 37 im Gehäuseteil 30 eingeschoben werden. Kurz vor Erreichen der Ruhestellung 11 fährt das mechanische Schlüsselteil 35 mit seinem hinteren Ende im Bereich seiner Auflaufschräge 85 gegen den Rasthaken 72 und stößt diesen gegen die Kraft der Feder 77 aus dem Führungskanal 37 hinaus. Der Rasthaken 72 schnappt dann bei Erreichen der Ruhestellung 11 durch das mechanische Schlüsselteil wieder in die Aussparung 75 ein und verrastet dort das mechanische Schlüsselteil 35.

Durch die manuelle Rücküberführung des mechanischen Schlüsselteils 35 in die Ruhestellung 11 ist der Zugkraftspeicher 50 wieder vorgespannt worden, so dass er bei einer erneuten Betätigung der Auslösetaste 70 das mechanische Schlüsselteil 35 wiederum aus seiner Ruhestellung 11 in seine Arbeitsstellung 15 überführen kann.

IPR2022-00412
Apple EX1053 Page 566

In den Fig. 9 und 10 ist nun ein weiteres Ausführungsbeispiel des erfindungsgemäßen Schlüssels dargestellt. In einem Gehäuseteil 30' ist wiederum ein mechanisches Schlüsselteil 35' in einem in dem Gehäuseteil 30' liegenden Führungskanal 37' verschieblich angeordnet. Der Führungskanal 37' wird gebildet aus den beiden Flächenwänden 40' und 41', die Abschnitten der Flächenseiten 38' und 39' der Gehäusegrundplatte 32' und des Gehäusedeckels 31' entsprechen. Die Seiten des Führungskanals 37' werden durch Wände 42' und 43' gebildet. In der Wand 43' ist eine Öffnung 44' vorgesehen, durch die ein als Zahnrad ausgeformtes Stellglied 47' hindurchgreift und die Zähne 62 des Zahnrades 47' in eine Zahnung 64 am mechanischen Schlüsselteil 35' eingreifen. Das Zahnrad 47' sitzt auf einer Achse 63, die in diesem Ausführungsbeispiel an der Gehäusegrundplatte 32' angeformt ist. Das Zahnrad 47' weist in seinem oberen Bereich einen Hohlraum auf, in dem ein Druckkraftspeicher 60, wie eine Spiralfeder angeordnet ist. Im unteren Umfangsbereich des Zahnrades unterhalb der Zahnung 62 ist eine Aussparung 76 vorgesehen, in die der Rasthaken 72' eines Hebels 71' hineinragt, wenn das mechanische Schlüsselteil 35' sich in seiner Ruhestellung oder seiner Arbeitsstellung befindet. Wie schon im vorausgehenden Ausführungsbeispiel ist der Hebel 71' über eine Auslösetaste 70' zu betätigen. Der Rasthaken steht wiederum unter der Kraft der Feder 77', die zwischen der rahmenseitigen Federsitz 78' und der Ansatzstelle 79' am Hebel 70' angeordnet ist. In Fig. 9 ist das mechanische Schlüsselteil 35' in seiner Arbeitsstellung 15 dargestellt. Strichpunktiert dargestellt ist ferner noch die Ruhestellung des mechanischen Schlüsselteils 35'.

An dem gehäuseteilseitigen Ende des mechanischen Schlüsselteils 35' ist eine Nase 48' in Richtung der Wand 42' an dem mechanischen Schlüsselteil 35' angeformt. Diese Nase 48' ist in einer Öffnung 46', die in der Wand 42' parallel zum Führungskanal 37' und der Ausschubrichtung 16 des mechanischen Schlüsselteils 35' verläuft, angeordnet. Durch die Nase 48' wird die Ausschubbewegung des mechanischen Schlüsselteils 35', die durch den Druckkraftspeicher 60 mittels des Zahnrades 47' auf das mechanische Schlüsselteil 35' übertragen wird, wenn die

IPR2022-00412
Apple EX1053 Page 567

Auslösetaste 70' gedrückt worden ist, begrenzt, da die Nase 48' beim Erreichen der Arbeitsstellung 15 gegen den Anschlag 49' fährt.

Zum Einfahren des mechanischen Schlüsselteils 35' muss wiederum die Auslösetaste 70' betätigt werden, so dass der Rasthaken 72' aus der Aussparung 76 herausfährt und derart eine Drehbewegung des Zahnrades 47' ermöglicht wird. Das mechanische Schlüsselteil 35' kann nun wieder in den Führungskanal 37' des Gehäuseteils 30' eingeschoben werden, wobei das Zahnrad 47' mitgedreht wird und derart der Druckkraftspeicher 60 bzw. die Spiralfeder wieder aufgezogen wird, um ein erneutes Ausfahren zu erlauben. Der Einschiebevorgang wird beendet, wenn die Nase 48' vor den Anschlag 54' läuft, der die Öffnung 46' an ihrem rückwärtigen Ende begrenzt. In der nun erreichten Ruhestellung 11 schnappt der Rasthaken 72' wieder in die Aussparung 76 am unteren Rand des Zahnrads 47' ein. Das mechanische Schlüsselteil 35' ist nunmehr in der Ruhestellung 11 verrastet. Das Verrasten des Rasthakens 72' in die Aussparung 76 am unteren Rand des Zahnrades 47' erfolgt also bei ein- und ausgeschobenem mechanischen Schlüsselteil. Dies bedeutet, dass eine Umdrehung des Zahnrades 47' gleich dem Hub des mechanischen Schlüsselteils sein muss.

Ein erneutes Ausfahren in die Arbeitsstellung 15 kann wiederum durch Betätigen der Auslösetaste 70' erfolgen, wodurch der Rasthaken 72' erneut aus der Aussparung 76 ausfährt und das Zahnrad 47', welches nunmehr freigegeben ist mit der Kraft der Spiralfeder 60 das mechanische Schlüsselteil 35' aus dem Führungskanal 37' hinausfährt und in die Arbeitsstellung 15 überführt.

In den Fig. 11 und 12 ist nun ein drittes Ausführungsbeispiel des erfindungsgemäßen Schlüssels wiedergegeben. Das mechanische Schlüsselteil 35'' ist in einem Gehäuseteil 30'' in einem Führungskanal 37'' angeordnet. Die Flächenwände 40'' des Führungskanals 37'' werden wiederum gebildet aus den Flächenseiten 38'' der Gehäusegrundplatte 32'' und der nicht dargestellten

IPR2022-00412
Apple EX1053 Page 568

Flächenseite des ebenfalls nicht dargestellten Gehäusedeckels. An den Schmalseiten des Führungskanals sind Wände 42'' und 43'' angeordnet, die bei diesem Ausführungsbeispiel jeweils einen Kanal 67 und einen Kanal 68 aufweisen. Die Wand 43'' weist eine längliche Öffnung 44'' auf, die parallel zur Ausschubrichtung 16 des mechanischen Schlüsselteils 35'' verläuft. Im hinteren Bereich des Gehäuseteils 30'' ist ein Druckkraftspeicher 60'' wie eine Spiralfeder angeordnet, die auf ein Zahnrad 65 einwirkt, welches drehbar auf einer Achse 63'' gelagert ist. Die Zahnung 62'' am Zahnrad 65 greift in Zahnöffnungen 66 eines Schubmittels 61, wie etwa eines Zahnriemens ein, der in den Kanälen 67 und 68, sowie um das Zahnrad 65 herum und an dem dort gegenüberliegenden Wandabschnitt 53'' geführt ist. Am vorderen Ende dieses Schubmittels/Zahnriemens 61 ist ein Stellglied 47'' angeordnet, mittels dessen eine vom Zahnriemen 61 ausgeübte Stellbewegung auf das mechanische Schlüsselteil 35'' übertragen werden kann. Am vorderen Ende des Zahnriemens 61 ist ebenfalls ein Sperrmittel 76' angeordnet, welches in der Ruhestellung 11 des mechanischen Schlüsselteils 35''an dem Rasthaken 72'' eines Hebels 71'' unter der Stellkraft des Druckkraftspeichers 60'' anliegt. Das Sperrmittel 76' liegt dabei über dem Wandabschnitt 53'' der Wand 47''.

Der Hebel 71'' ist auf einer Achse 81'' verschwenkbar gelagert. Er weist an seinem zweiten Ende eine Auslösetaste 70'' auf, mittels derer der Rasthaken 72'' entgegen der Federkraft einer Feder 77'', die an den Ansatzstellen 79'' und 78'' zwischen dem vorderen Arm des Hebels 71'' und der gehäuseseitigen Wand 43'' angeordnet ist.

In Fig. 11 ist der erfindungsgemäße Schlüssel in der Ruhestellung 11 des mechanischen Schlüsselteils 35'' dargestellt. Das mechanische Schlüsselteil 35'' liegt dabei gänzlich in dem Führungskanal 37'' gehäuseseitig hinter der Schlüsselstellung 12.

Wird die Auslösetaste 70'' betätigt, und der Hebel 71'' entgegen der Kraft der Feder 77'' verschwenkt, so gibt der Rasthaken 72'' das Sperrmittel/Sperrglied 76' frei. Hierdurch kann nun das Schubmittel 61 mit dem daran angeordneten Stellglied 47'' aufgrund des von dem Druckkraftspeicher 60'' ausgeübten Bewegungsmomentes das von dem Druckkraftspeicher 60'' auf das Zahnrad 65 und von diesem über die Zahnung 62'' und die Zahnöffnung 66 auf das Schubmittel 61 übertragen wird in Ausschubrichtung 16 auf die Schlüsselöffnung 12 zubewegt, wodurch der über das Stellglied 47'' betätigte mechanische Schlüsselteil 35'' aus dem Gehäuseteil 30'' heraus in seine Arbeitsstellung 15 verfahren wird. Beim Erreichen der Arbeitsstellung 15 fährt die Nase 48'' des Stellgliedes 47'' vor einem Anschlag 49'', der am Ende der Öffnung 44'' angeordnet ist. Ein Sperrmittel 76'', welches in Ausschubrichtung mit einer Auflaufschräge versehen ist, ist bei der Ausschubbewegung hinter den Rasthaken 72'' gefahren, und verhindert nun über das Schubmittel 61 und das Stellglied 47'' ein Wiederhereinfahren des mechanischen Schlüsselteils 35''.

Bei erneuter Betätigung der Auslösetaste 70'' wird das Sperrmittel 76'' wieder freigegeben und es kann das mechanische Schlüsselteil 35'' wieder manuell in den Führungskanal 37'' im Gehäuseteil 30'' hineingeschoben werden. Hierdurch bewegt sich das Schubmittel 61 in reverser Richtung am Zahnrad 65 vorbei, welches hierdurch wieder bewegt wird, so dass die an dem Zahnrad 65 angelenkte und in dem Zahnrad 65 befindliche Spiralfeder 60'' mit der Einschubbewegung des mechanischen Schlüsselteils 35'' wieder gespannt wird. Kurz vor Erreichen der Ruhestellung 11 durch das mechanische Schlüsselteil 35'' fährt das Sperrmittel/Sperrglied 76' mit seiner Auflaufschräge gegen den Rasthaken 72'' und schiebt sich an diesem vorbei. Der Rasthaken 72'' fährt unter der Krafteinwirkung der Feder 77'' wieder hinter das Sperrmittel/Sperrglied 76' und blockiert ein Wiederherausfahren des mechanischen Schlüsselteils 35'' unter der Krafteinwirkung des Druckkraftspeichers/Spiralfeder 60''. Um ein zu weites Einschieben des mechanischen Schlüsselteils 35'' zu vermeiden, ist am hinteren Ende der Öffnung

IPR2022-00412
Apple EX1053 Page 570

44'' ein Anschlag 54'' vorgesehen, gegen den die Nase 48'' des Stellgliedes 47'' beim Einschieben des mechanischen Schlüsselteiles 35'' fährt. Gleichzeitig läuft das Sperrmittel 76'' gegen einen Anschlag 56, der am Ende der Wand 42'' liegt.

Neben den hier dargestellten Ausführungsbeispielen sind noch weitere Ausführungsformen denkbar. So sind insbesondere Ausführungsformen denkbar, bei denen die Schlüsselöffnung durch ein weiteres Mittel verschließbar ist, wenn das mechanische Schlüsselteil sich gänzlich im Führungskanal befindet.

Weiterhin ist z.B. eine Ausführungsform denkbar, bei der eine linear wirkende und linear verstellbare Druckfeder direkt auf ein Stellglied, wie z.B. das Stellglied 47 oder 47'' wirkt und derart ein mechanischer Schlüsselteil aus einem Gehäuseteil herausgeschoben werden kann. Eine solche linear wirkende Druckfeder kann z.B. in einem weiteren Führungskanal benachbart zum Führungskanal für das mechanische Schlüsselteil angeordnet sein, oder aber eine derartige Steifigkeit aufweisen, dass eine Führung des Federelementes nicht notwendig ist.

Ebenso könnte das mechanische Schlüsselteil über elektrisch angesteuerte solenoide oder durch hydraulisch wirkende Druckkraftspeicher aus dem Gehäuseteil ausgeschoben werden. Ebenso können anstelle einer Verrastung auch reibschlüssige Bremsmittel vorgesehen sein, die das mechanische Schlüsselteil jeweils in seinen Stellungen hält.

Es versteht sich ebenfalls, dass die Verbindungsmittel zwischen dem elektrischen Gehäuseteil und dem mechanischen Gehäuseteil auch anders als bei dem ersten Ausführungsbeispiel angeordnet sein können. So konnten die Nuten 27 und die Verrastmittelvorsprünge 28 auch in den Gehäusegrundplatten 32, 32', 32'' der die Schlüsselmechanik enthaltenden zweiten Gehäuseteile angeordnet sein. Die Schwalbenschwanzzapfen 23

IPR2022-00412
Apple EX1053 Page 571

müssten dann in den Gehäusegrundplatten 22 der, die Elektronik enthaltenden ersten Gehäuseteile angeordnet sein.

IPR2022-00412
Apple EX1053 Page 572

Bezugszeichenliste:

10 Schlüssel
11 Ruhestellung
12 Schlüsselöffnung

14 Ebene
15 Arbeitsstellung
16 Ausschieberichtung / Ausfuhrrichtung
17 Demontagerichtung
18 Montagerichtung
19 Öse
20 erstes Gehäuseteil mit Schlüsselelektronik
21 Gehäusedeckel erstes Gehäuseteil
22 Gehäusegrundplatte erstes Gehäuseteil
23 Batteriefachdeckel
24 Batterie
25 Elektronikbauteile
26 Tastfelder
27 Nut in der Gehäusegrundplatte
28 Verrastmittelvorsprung
29 Schraubmittel
30 zweites Gehäuseteil mit Schlüsselmechanik
30′ zweites Gehäuseteil mit Schlüsselmechanik
30′′ zweites Gehäuseteil mit Schlüsselmechanik
31 Gehäusedeckel zweites Gehäuseteil

31' Gehäusedeckel zweites Gehäuseteil
32 Gehäusegrundplatte
32' Gehäusegrundplatte
32'' Gehäusegrundplatte
33 Schwalbenschwanzzapfen
34 Frontteil der Gehäusegrundplatte
35 Schlüsselteil
35' Schlüsselteil
36 Gehäuseinnenraum (zweites Gehäuseteil)
37 Führungskanal
37' Führungskanal
37'' Führungskanal
38 Flächenseite
38' Flächenseite
38'' Flächenseite
39 Flächenseite
39' Flächenseite
40 Flächenwand
40' Flächenwand
40'' Flächenwand
41 Flächenwand
41' Flächenwand
42 Wand
42' Wand
42'' Wand
43 Wand
43' Wand
43'' Wand
44 Längsöffnung
44' Öffnung

IPR2022-00412
Apple EX1053 Page 574

44'' Längsöffnung
45 Öffnung
46 Öffnung
46' Öffnung
47 Stellglied
47' Stellglied / Zahnrad
47'' Stellglied
48 Nase
48' Nase
48'' Nase
49 Anschlag (Arbeitsstellung)
49' Anschlag (Arbeitsstellung)
49'' Anschlag (Arbeitsstellung)
50 Zugkraftspeicher
51 Zugmittel
52 Umlenkteil
53 Führungswand
53'' Wandabschnitt
54 Anschlag (Ruhestellung)
54' Anschlag (Ruhestellung)
54'' Anschlag (Ruhestellung)
55 Anschlag für Sperrmittel 76'
56 Anschlag für Sperrmittel 76''
60 Druckkraftspeicher
60'' Druckkraftspeicher
61 Schubmittel
62 Zähne am Stellglied 47'
62'' Zähne am Zahnrad 65
63 Achse
63'' Achse

IPR2022-00412
Apple EX1053 Page 575

64 Zahnung am Schlüssel 35' /Schubmittel
65 Zahnrad / Schubmittel
66 Zahnöffnung / Schubmittel 61
67 Kanal
68 Kanal
70 Auslösetaste (Auslösemittel)
70' Auslösetaste (Auslösemittel)
70'' Auslösetaste (Auslösemittel)
71 Hebel
71' Hebel
71'' Hebel
72 Rasthaken von Hebel 71
72' Rasthaken von Hebel 71
72'' Rasthaken von Hebel 71
73 Hebel
74 Rasthaken von Hebel 73
75 Sperrmittel / Aussparung
75'' Sperrmittel
76 Sperrmittel / Aussparung
76' Sperrmittel
76'' Sperrmittel
77 Druckmittel / Feder
77' Druckmittel / Feder
77'' Druckmittel / Feder
77''' Druckmittel / Feder
78 Federsitz
78' Federsitz
78'' Federsitz
78''' Federsitz
79 Ansatzstelle

79‘ Ansatzstelle

79‘‘ Ansatzstelle

79‘‘‘ Ansatzstelle

81 Hebelachse

81‘ Hebelachse

81‘‘ Hebelachse

83 Hebelachse

84 Berührungsstelle

85 Auflaufschräge

Patentansprüche :

1. Schlüssel, insbesondere für Kfz, mit einem Gehäuseteil (30, 30', 30'') und einem daran angeordneten mechanischen Schlüsselteil (35, 35', 35''),

bei dem wenigstens ein schließwirksamer Teil des Schlüsselteils (35, 35', 35'') mittels einer Mimik (47-47'', 50, 51, 52, 60, 60'', 61, 62, 62'', 64, 65, 66) von einer Ruhestellung (11) in eine Arbeitsstellung (15) zu überführen ist, in der der Schlüssel (10) zur mechanischen Betätigung eines Schlosses benutzt werden kann,

wobei zur Aktivierung der Mimik (47-47'', 50, 51, 52, 60, 60'', 61, 62, 62'', 64, 65, 66) ein manuell zu betätigendes Auslösemittel (70) vorgesehen ist,

und das Schlüsselteil (35, 35', 35'') in der Arbeitsstellung (15) im wesentlichen bewegungsstarr ist,

dass das Schlüsselteil (35, 35', 35'') in seiner Ruhestellung (11) in einem Gehäuseinnenraum (36) angeordnet ist,

und dass das Schlüsselteil (35, 35', 35'') nach einer Betätigung des Auslösemittels (70) mittels der Mimik (47-47'', 50, 51, 52, 60, 60'', 61, 62, 62'', 64, 65, 66) von seiner Ruhestellung (11) im Gehäuseinnenraum (36) durch eine laterale Verschiebung aus dem Gehäuseteil (30, 30', 30'') heraus, in die Arbeitsstellung (15) zu überführen ist,

IPR2022-00412
Apple EX1053 Page 578

und in dem Gehäuseinnenraum (36) Mittel (37, 40, 41, 42, 43) angeordnet sind, durch die das Schlüsselteil (35, 35', 35'') bei der Längsverschiebung geführt ist,

dadurch gekennzeichnet,

dass die Mimik (47-47'', 50, 51, 52, 60, 60'', 61, 62, 62'', 64, 65, 66) einen Zug- (50) oder Druckkraftspeicher (60) umfasst, der indirekt über ein Zug- (51) oder Schubmittel (61, 64, 65, 66) an dem Stellglied (47) angreift.

2. Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass in dem Gehäuseteil (30, 30', 30'') in Ausschubrichtung (16) des Schlüsselteils (35, 35', 35'') eine Schlüsselöffnung (12) angeordnet ist, die formschlüssig zur Außenkontur des Schlüsselteils (35, 35', 35'') ausgebildet ist.

3. Schlüssel nach einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, dass der Gehäuseinnenraum (36) des Gehäuseteils (30, 30', 30'') über ein an der Schlüsselöffnung (12) angeordnetes Verschlussmittel von dem, das Gehäuseteil (30, 30', 30'') umgebenden Außenraum abgeschlossen ist.

4. Schlüssel nach Anspruch 1, dadurch gekennzeichnet, daß die Mittel zur Führung des Schlüsselteils (35, 35', 35'') einen Führungskanal (37) umfassen.

5. Schlüssel nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass das, den mechanischen Schlüsselteil (35, 35', 35'') und die Mimik (47 - 47'', 50, 51, 52, 60, 60'', 61, 62, 62'', 64, 65, 66) beherbergende Gehäuseteil (30, 30', 30'') wenigstens zwei, im wesentlichen parallel zueinander verlaufende Flächenseiten (38, 38', 39, 39'') aufweist, und diese Flächenseiten (38, 38', 39, 39'') zu zwei Seiten die Flächenwände (40, 40', 40'', 41, 41') des Führungskanals (37) bilden.

IPR2022-00412
Apple EX1053 Page 579

6. Schlüssel nach einem der Ansprüche 1 und 5, dadurch gekennzeichnet, dass im wesentlichen senkrecht zu den Flächenwänden (40, 40′, 40′′, 41, 41′) zwei im wesentlichen parallel verlaufende Wände (42, 42′, 42′′, 43, 43′, 43′′) den Führungskanal (37) seitlich begrenzen.

7. Schlüssel nach einem der Ansprüche 1 und 6, dadurch gekennzeichnet, dass wenigstens eine Wand (42, 42′, 42′′, 43, 43′, 43′′) des Führungskanals eine Öffnung (44, 44', 44'') aufweist durch den ein, auf das mechanische Schlüsselteil (35, 35′, 35‘‘) einwirkendes Stellglied (47, 47', 47'') der Mimik die Wand (42, 42′, 42′′, 43, 43′, 43′′) durchgreift.

8. Schlüssel nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass die Öffnung (44, 44'') im wesentlichen linear und parallel zur Ausschiebrichtung (16) des mechanischen Schlüsselteils (35, 35′, 35‘‘) verläuft.

9. Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass ein Endanschlag (49, 49'') vorgesehen ist, gegen den eine am Schlüsselteil (35, 35′, 35‘‘) angeordnete Nase (48, 48', 48'') zur Begrenzung des Ausschubwegs aufläuft.

10. Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass der mechanische Schlüsselteil (35, 35′, 35‘‘) durch Rastmittel (71 - 71′′, 72 - 72′′, 73, 74, 75, 76-76′′) in seiner Ruhe- (11) und in seiner Arbeitsstellung (15) bewegungsstarr gehalten ist.

11. Schlüssel nach einem der Ansprüche 1 und 10, dadurch gekennzeichnet, dass die Rastmittel (71 - 71′′, 72 - 72′′, 73, 74, 75, 76-76′′) durch Betätigung des Auslösemittels (70 - 70′′) freigegeben werden.

IPR2022-00412
Apple EX1053 Page 580

12. Schlüssel nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, dass die Rastmittel wenigstens einen Hebel (71 - 71'', 73) mit mit wenigstens einem Rasthaken (72 - 72'', 74) umfassen, der in der Arbeits- (15) und/oder Ruhestellung (11) jeweils auf ein Sperrmittel (75 - 75'', 76, 76') einwirkt.

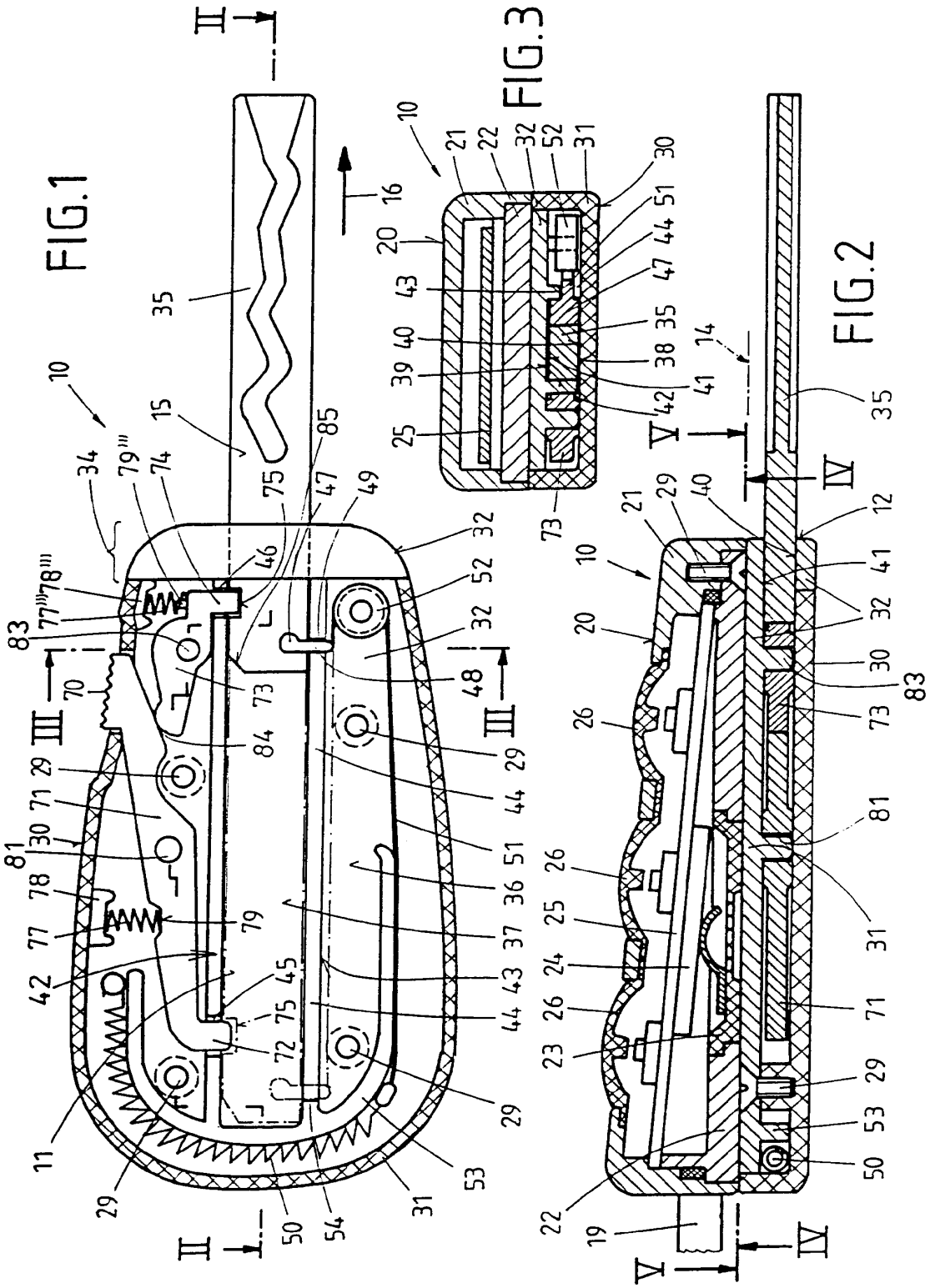
13. Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass der Zugkraftspeicher (50) über ein Zugmittel (51) an dem Stellglied (47) angreift, wobei der Zugweg des Zugmittels (51) und des Zugkraftspeichers (50) durch Umlenkung des Zugmittels (51) an einem Umlenkteil (52), insbesondere einer Umlenkrolle, vergrößert ist.

14. Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass der Druckkraftspeicher (60) über Schubmittel (61, 64, 65, 66) an dem Stellglied (47'') angreift.

15. Schlüssel, nach Anspruch 1, dadurch gekennzeichnet, dass zwei in sich abgeschlossene Gehäuseteile (20, 30; 20', 30'; 20'', 30'') aneinander angeordnet sind, wobei das erste Gehäuseteil (20, 20', 20'') eine Schlüsselelektronik (25, 24), und das zweite Gehäuseteil (30; 30'; 30'') einen mechanischen Schlüsselteil (35, 35', 35'') und eine Mimik (47 - 47'', 50, 51, 52, 60, 60'', 61, 62, 62'', 64, 65, 66) beinhaltet, und bei dem die beiden Gehäuseteile (20, 30; 20', 30', 20'', 30'') entlang einer einzelnen, im wesentlichen planaren Ebene (14) reversibel aneinander festgelegt sind.

16. Schlüssel nach Anspruch 15, dadurch gekennzeichnet, dass im Bereich der planaren Ebene (14) Verbindungsmittel (28, 30) an den Gehäuseteilen 20, 30; 20', 30'; 20'', 30'') angeordnet sind, mittels derer die Gehäuseteile (20, 30; 20', 30'; 20'', 30'') reversibel aneinander festgelegt sind.

IPR2022-00412
Apple EX1053 Page 581



IPR2022-00412
Apple EX1053 Page 582

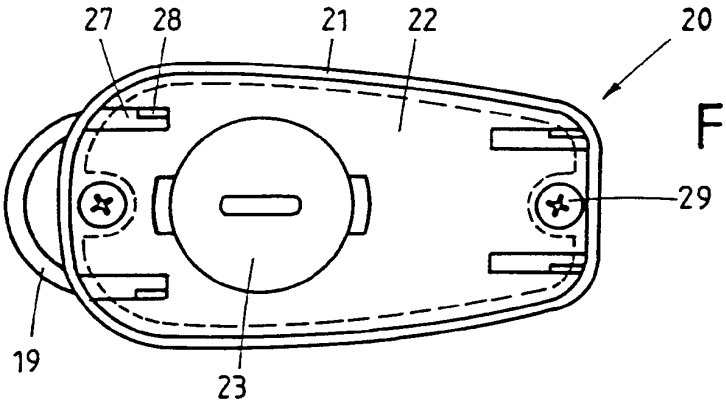


FIG.4

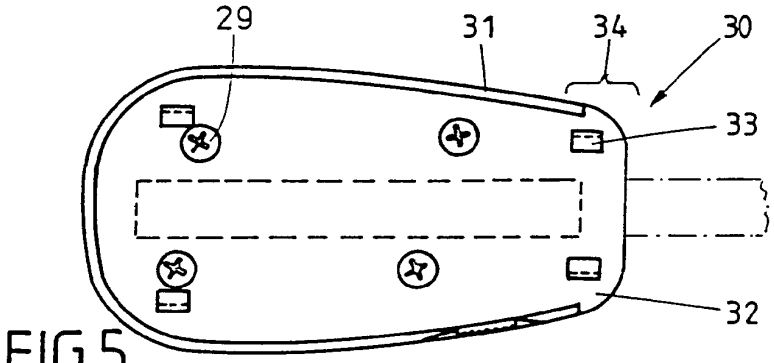
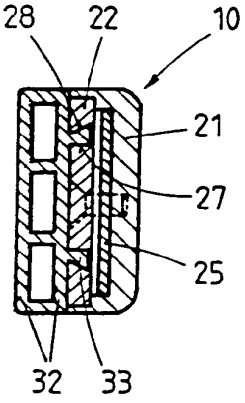


FIG.5

FIG.8



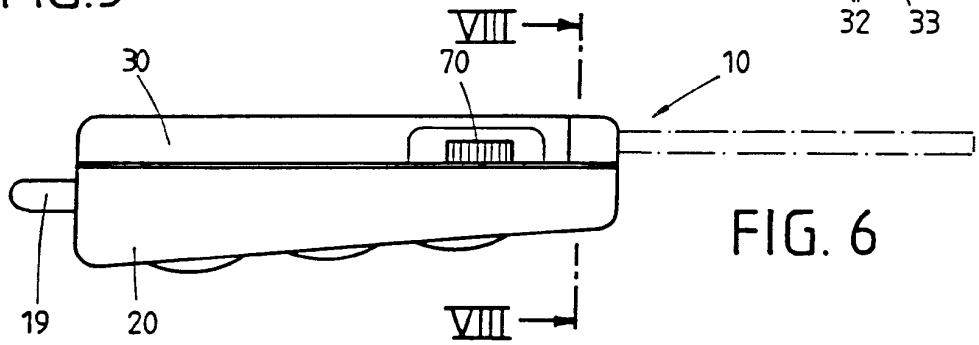


FIG. 6

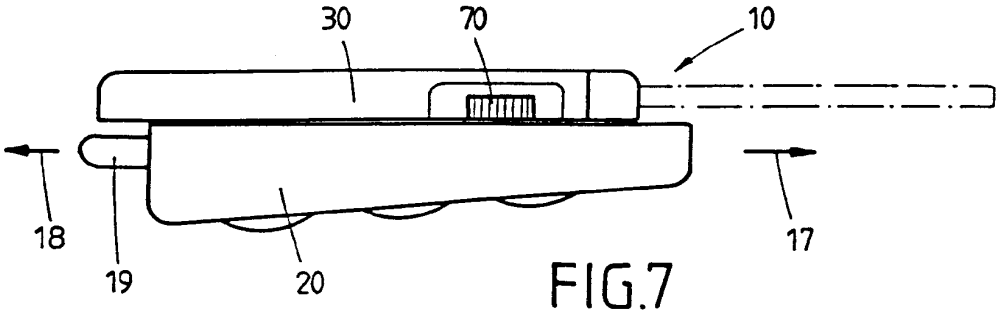


FIG.7

FIG.9

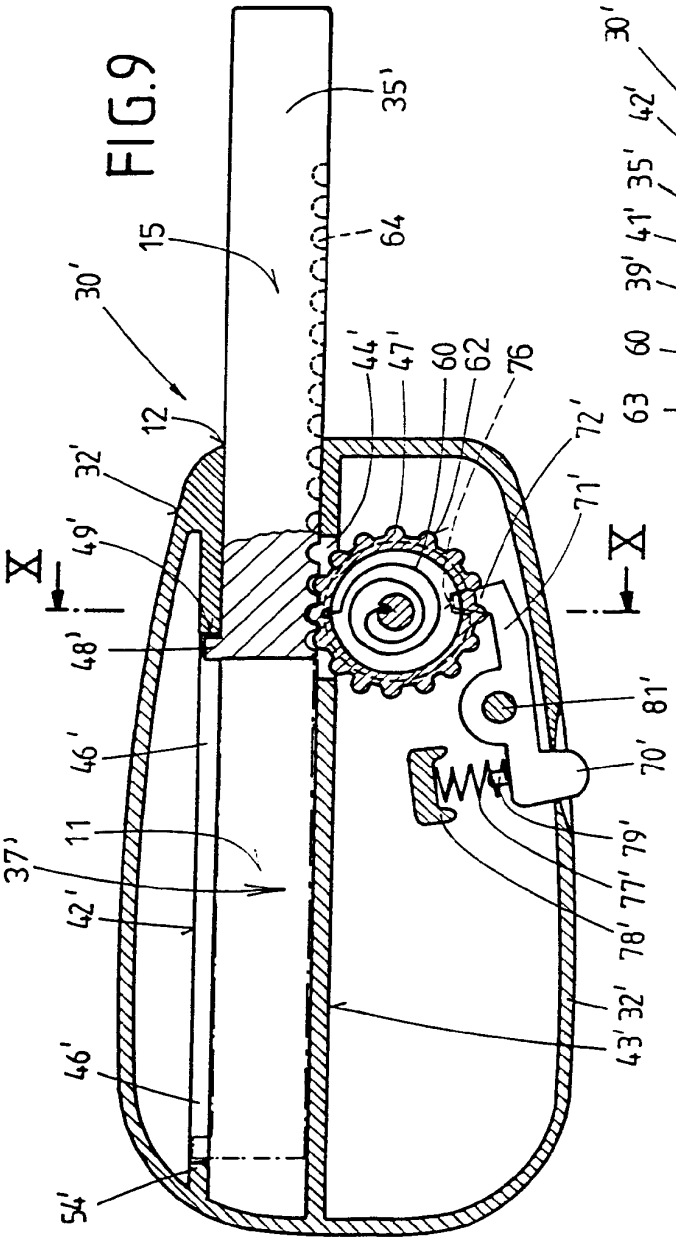
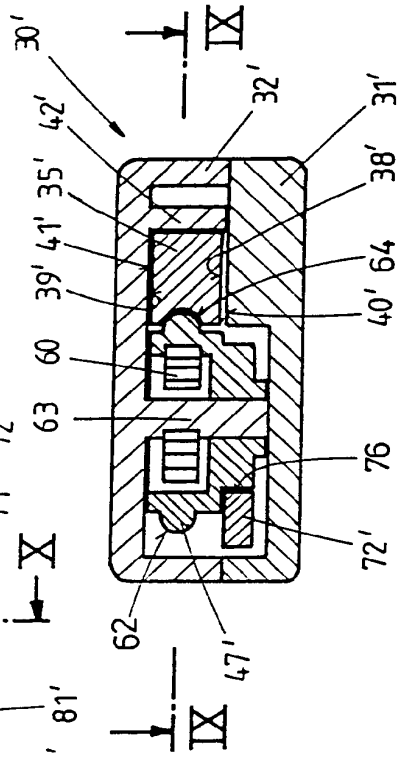

35'
15
64
30'
12
32'
49'
48'
46'
11
37'
42'
46'
54'
44'
47'
60
62
76
72'
71'
81'
70'
79'
77'
78'
43'
X
X

FIG.10


30'
IX
IX
42'
32'
31'
35'
38'
41'
39'
64
40'
60
63
76
72'
62
47'

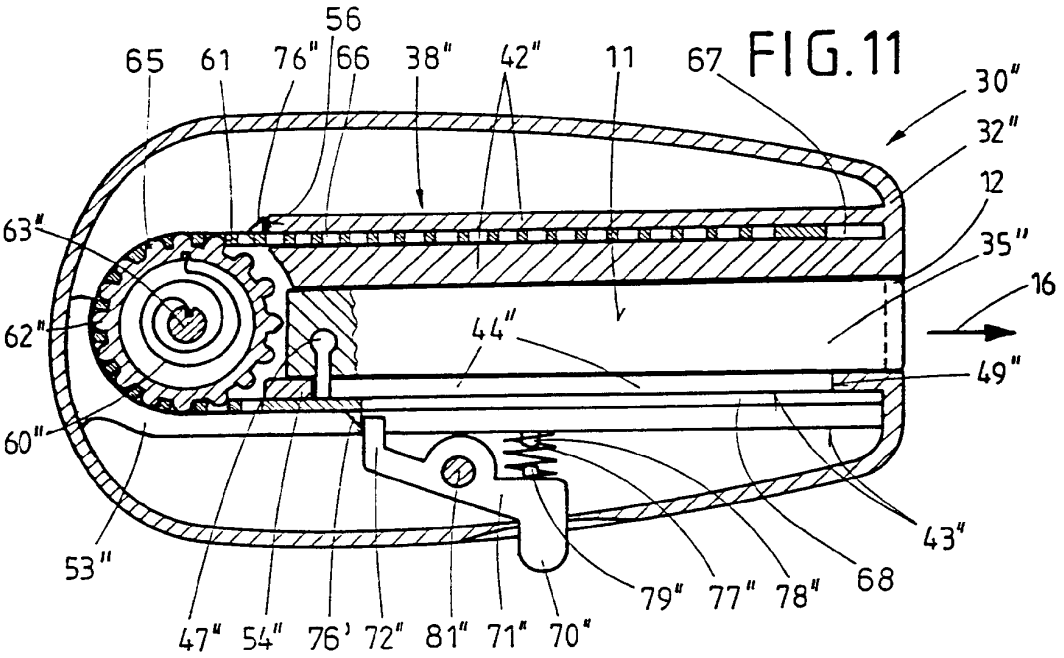


FIG.11

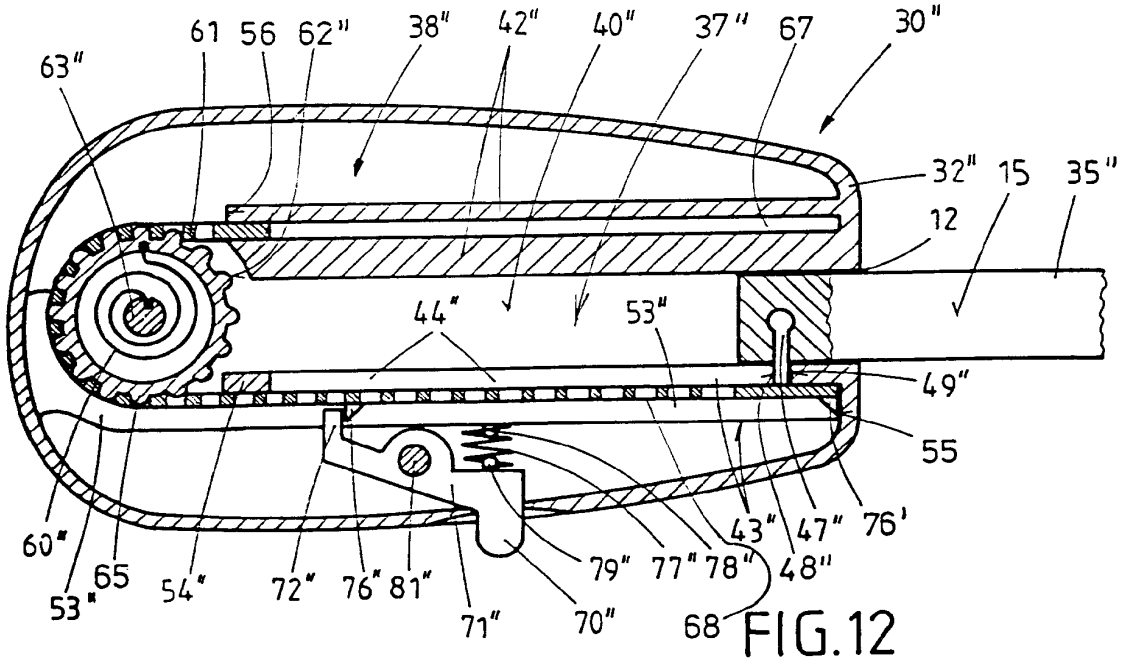


FIG.12

IPR2022-00412
Apple EX1053 Page 585

INTERNATIONAL SEARCH REPORT

Interr. nal Application No
PCT/EP 00/11504

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 E05B19/04 A45C11/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 A45C E05B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	DE 199 12 749 C (VALEO GMBH & CO SCHLIESSYST KG) 2 November 2000 (2000-11-02) column 3, line 35 - line 59; figure ---	1-5, 7-12, 14-16
X	US 2 690 666 A (MORRIS ENGEL ET AL.) 5 October 1954 (1954-10-05) cited in the application column 4, line 7 - line 51; figure ---	1,2,4-6, 9-12
X	US 3 328 986 A (THEODORE RALTON) 4 July 1967 (1967-07-04) column 2, line 35 - line 62; figure ---	1,2,4-6, 9-11,14
A	FR 2 597 537 A (PEUGEOT) 23 October 1987 (1987-10-23) page 3, line 4 - line 24; figures 1,3,4 -----	15

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 April 2001	20/04/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Pieracci, A

Form PCT/ISA/210 (second sheet) (July 1992)

IPR2022-00412
Apple EX1053 Page 586

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interr. nal Application No
PCT/EP 00/11504

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19912749 C	02-11-2000	NONE	
US 2690666 A	05-10-1954	NONE	
US 3328986 A	04-07-1967	NONE	
FR 2597537 A	23-10-1987	NONE	

Form PCT/ISA/210 (patent family annex) (July 1992)

INTERNATIONALER RECHERCHENBERICHT

Intern. nales Aktenzeichen
PCT/EP 00/11504

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 E05B19/04 A45C11/32

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 A45C E05B

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
P,X	DE 199 12 749 C (VALEO GMBH & CO SCHLIESSYST KG) 2. November 2000 (2000-11-02) Spalte 3, Zeile 35 - Zeile 59; Abbildung	1-5, 7-12, 14-16
X	US 2 690 666 A (MORRIS ENGEL ET AL.) 5. Oktober 1954 (1954-10-05) in der Anmeldung erwähnt Spalte 4, Zeile 7 - Zeile 51; Abbildung	1,2,4-6, 9-12
X	US 3 328 986 A (THEODORE RALTON) 4. Juli 1967 (1967-07-04) Spalte 2, Zeile 35 - Zeile 62; Abbildung	1,2,4-6, 9-11,14
A	FR 2 597 537 A (PEUGEOT) 23. Oktober 1987 (1987-10-23) Seite 3, Zeile 4 - Zeile 24; Abbildungen 1,3,4	15

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
10. April 2001	20/04/2001
Name und Postanschrift der Internationalen Recherchenbehörde Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bevollmächtigter Bediensteter Pieracci, A

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

IPR2022-00412
Apple EX1053 Page 588

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internales Aktenzeichen
PCT/EP 00/11504

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 19912749	C	02-11-2000	KEINE	
US 2690666	A	05-10-1954	KEINE	
US 3328986	A	04-07-1967	KEINE	
FR 2597537	A	23-10-1987	KEINE	

IPR2022-00412
Apple EX1053 Page 589

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 May 2001 (31.05.2001)

PCT

(10) International Publication Number
WO 01/39102 A1

(51) International Patent Classification[7]: G06K 7/00

(21) International Application Number: PCT/IT00/00429

(22) International Filing Date: 25 October 2000 (25.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
TO99A001020 22 November 1999 (22.11.1999) IT

(71) Applicant *(for all designated States except US)*: **EUTRON INFOSECURITY S.R.L.** [IT/IT]; Via Gandhi, 12, I-24048 Curnasco di Treviolo (IT).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **CASSIA, Lucio** [IT/IT]; c/o Eutron Infosecurity S.R.L., Via Gandhi, 12, I-24048 Curnasco di Treviolo (IT). **LEIDI, Michele** [IT/IT]; c/o Eutron Infosecurity S.R.L., Via Gandhi, 12, I-24048 Curnasco di Treviolo (IT).

(74) Agent: **GARAVELLI, Paolo**; c/o A.Bre.Mar. S.r.l., Via Servais, 27, I-10146 Torino (IT).

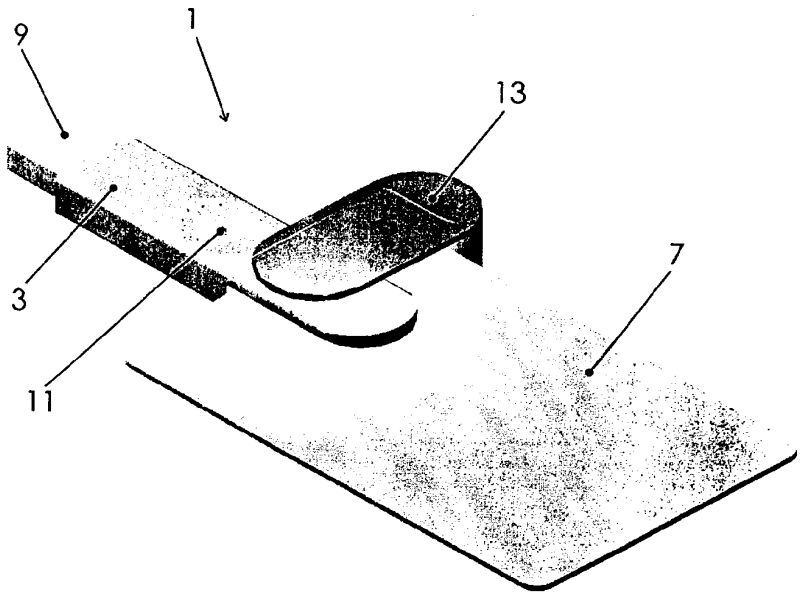
(81) Designated States *(national)*: AE, AL, AU, BA, BB, BG, BR, CA, CN, CR, CU, CZ, DM, EE, GD, GE, HR, HU, ID, IL, IN, IS, JP, KP, KR, LC, LK, LR, LT, LV, MA, MG, MK, MN, MX, NO, NZ, PL, RO, SG, SI, SK, TR, TT, UA, US, UZ, VN, YU, ZA.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: PORTABLE READER FOR SMART CARDS



(57) Abstract: A portable reader (1) for smart cards (7) is described that comprises: a support body (3) containing at least one slot (5) for inserting and reading a smart card (7); interface means (9) connected to the support body (3); interface means (9) connected to the support body (3); means (13) for keeping and aligning the smart card (7); and a managing microprocessor contained inside the support body (3) and connected to the interface means (9) and the reading means for smart cards (7).

WO 01/39102 A1

PORTABLE READER FOR SMART CARDS

The present invention refers to a portable reader for intelligent cards of the type commonly known as "smart cards".

Smart cards are nowadays rather widespreaded given their practical easiness of use: in fact, they allow, through microprocessors realised on integrated circuit chips obtained therein, to store a very high amount of data and therefore they can be used in applications such as different types of credit cards, cryptographic cards and future applications such as identity cards or electronic health cards.

For the purpose for which they are provided, such smart cards are adapted to communicate (that is, to transmit and receive) data through communication standards that are well-known at world level, such as the 7816 Standard. To realise such communication, the intelligent card is put in contact with a card reading device, which is equipped with suitable slots in which the card is

IPR2022-00412
Apple EX1053 Page 591

inserted, such slots containing a certain number of contacts that read the card data and communicate them to the microprocessor managing the card reader. Card readers are currently available on the market that are realised in the shape of boxes whose sizes are about 15 x 10 cm, that are statically connected to different types of data processing and transmitting systems. Such smart card readers are therefore with a relatively high encumbrance and due to their nature they are provided fixed in well-defined positions. On the market, there are currently no smart card readers that are portable and with small sizes.

Object of the present invention is solving the above prior-art problems, by providing a portable reader for smart cards that is of very reduced sizes and therefore can be easily transported and used by end users for any type of application.

A further object of the present invention is providing a portable reader that is equipped with such interface means as to allow it to widely and immediately use all smart cards with which a user can be equipped: for such purpose, the reader is equipped with means allowing it to be connected to a common Universal Serial Bus (USB) port of a

IPR2022-00412
Apple EX1053 Page 592

computer.

The above and other objects and advantages of the invention, as will appear from the following description, are obtained by a portable reader for smart cards as claimed in Claim 1. Preferred embodiments and non-trivial variations of the present invention are claimed in the dependent Claims.

The present invention will be better described by some preferred embodiments thereof, given as a non-limiting example, with reference to the enclosed drawings, in which:

- Figure 1 is a perspective view of an embodiment of a portable reader according to the present invention coupled with a smart card in the operating position;
- Figure 2 is a perspective view of the reader in Fig. 1 in the transport position;
- Figure 3 is a top view of the operating configuration in Fig. 1; and
- Figure 4 is a top view of the reader in Fig. 2.

With reference to the Figures, a preferred embodiment of the portable reader 1 for intelligent cards is shown, such cards being commonly known as

IPR2022-00412
Apple EX1053 Page 593

"smart cards".

The portable reader 1 for smart cards of the present invention substantially comprises a support body 3 shaped as an elongated box, comprising at one end thereof at least one slot 5 for inserting and reading therein a smart card 7. For such purpose, the slot 5 is equipped with reading means (not shown) for smart cards 7, that are commonly known and are composed of a plurality (usually six) of contacts that carry connection wires to a managing microprocessor (also not shown) contained inside the support body 3.

Such managing microprocessor is preferably realised through an integrated circuit chip and contains inside it all the necessary logics for receiving and transmitting data to the smart card 7 to which it is connected.

In order to communicate with the outside world the data obtained from a connected smart card 7, the portable reader 1 of the invention is further equipped with interface means 9 connected to the support body 3 and to the managing microprocessor; commonly, such interface means 9 are adapted to be connected to a common USB port of a computer, in order to be able to realise a connection with the

IPR2022-00412
Apple EX1053 Page 594

most widely known external managing networks (Internet, Intranet, etc.).

Moreover, the portable reader 1 of the invention comprises means 13 for keeping and aligning the smard card 7, that, in the practical embodiment shown, are composed of a bracket shaped as an elongated C and hinged to the support body 3 in order to have:

a) an operating position in which the keeping and aligning means 13 are perpendicular to the support body 3 to keep the card 7 in contact with the reader 1 and to align the card 7 with the reading means (as can be clearly shown in Fig.s 1 and 3; and

b) a rest position in which the keeping and aligning means 13 are aligned with the support body 3 allowing to transport and store the reader 1 (as can be clearly seen in Fig.s 2 and 4).

Finally, the portable reader 1 of the invention can be further equipped with means 11 that enable grasping the support body 3 by means of two fingers of an hand, such as for example the depression 11 shown in the different Figures.

A portable reader 1 has thereby been realised

IPR2022-00412
Apple EX1053 Page 595

that can be placed and stored in any suitable place and that can be easily transported and connected to USB ports: in this way, by arranging a reader whose overall sizes are on the order of 3 cm, it is possible to realise a flexible solution wherein each smart card with which a user is equipped can be immediately and easily connected and activated for the outside world to perform flexible and powerful applications.

Some preferred embodiments of the invention have been disclosed, but obviously they are subjected to further modifications and variations within the same inventive idea. For example, the reader 1 of the invention can be realised on a personal identification device like the one marketed by the Assignee of the present invention, containing in a single configuration the functionalities of personal identification, encrypted data transmission and smart cards reading. Otherwise, the reader 1 of the present invention can be pre-arranged in a stand-alone configuration according to application needs, guaranteeing at any rate an efficient solution as regards the practical comfort of the shape and portability of the reader 1 itself.

IPR2022-00412
Apple EX1053 Page 596

CLAIMS

1. Portable reader (1) for smart cards (7), characterised in that it comprises:
   - a support body (3) containing at least one slot (5) for inserting and reading a smart card (7), said slot (5) being equipped with reading means for smart cards (7);
   - interface means (9) connected to said support body (3);
   - means (13) for keeping and aligning said smart card (7); and
   - a managing microprocessor contained inside said support body (3) and connected to said interface means (9) and said reading means for smart cards (7).
2. Portable reader (1) according to Claim 1, characterised in that said interface means (9) are adapted to be connected to an USB port.
3. Portable reader (1) according to Claim 1, characterised in that said reading means for smart cards (7) are composed of a plurality of contacts carrying connection wires to said managing microprocessor.
4. Portable reader (1) according to Claim 3,

IPR2022-00412
Apple EX1053 Page 597

characterised in that said contacts are equal to six.

5. Portable reader (1) according to Claim 1, characterised in that said keeping and aligning means (13) are composed of an elongated-C-shaped bracket, said bracket being hinged to said support body (3) in order to have:

   a. an operating position in which said keeping and aligning means (13) are perpendicular to said support body (3) to keep the card (7) in contact with said reader (1) and to align the card (7) with said reading means; and

   b. a rest position in which said keeping and aligning means (13) are aligned with said support body (3) allowing to transport and store said reader (1).

6. Portable reader (1) according to Claim 1, characterised in that it is further equipped with means (11) that enable grasping said support body (3) by means of two fingers of an hand.

IPR2022-00412
Apple EX1053 Page 598

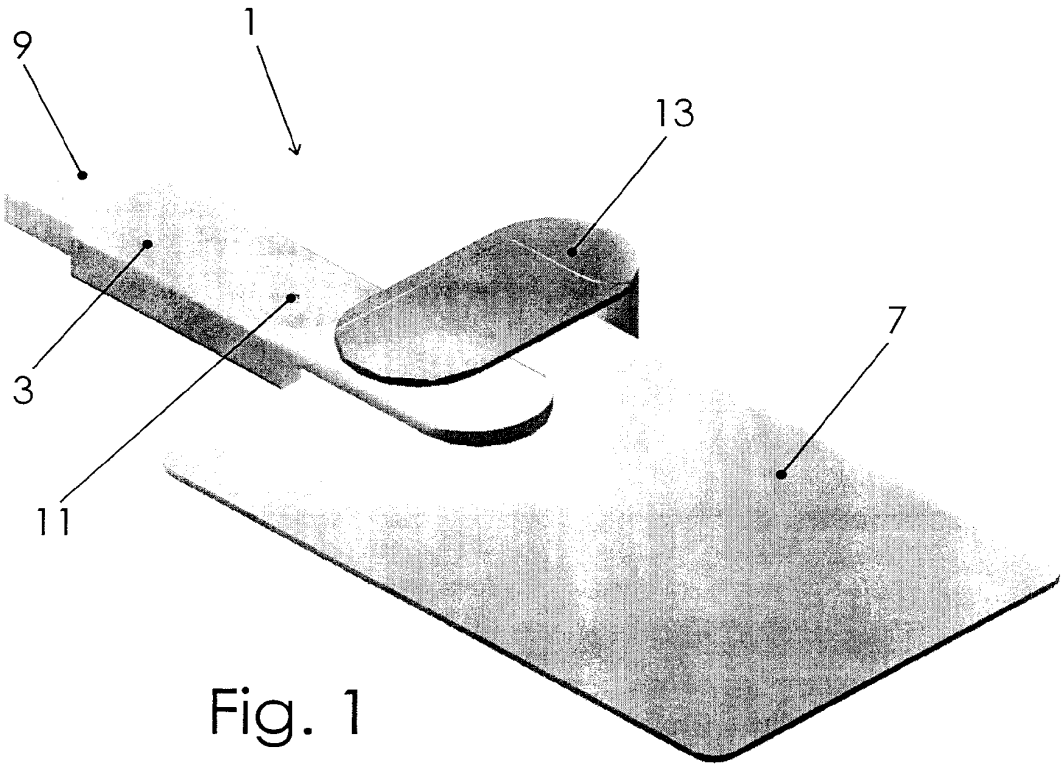


Fig. 1

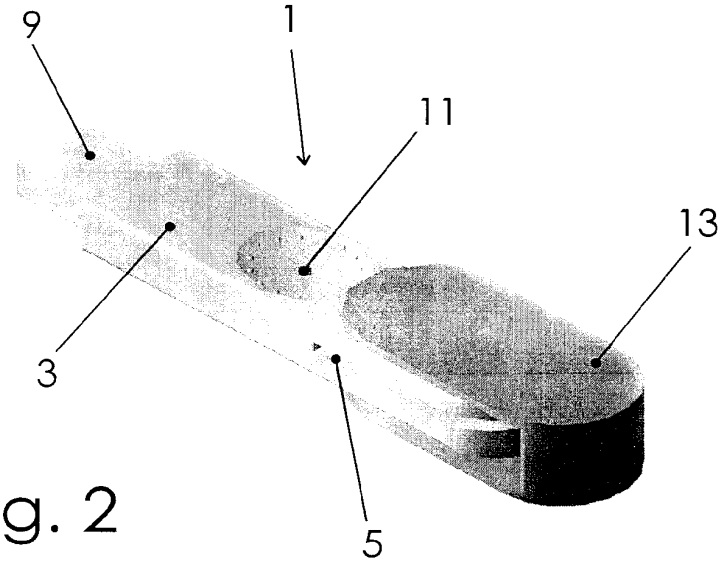


Fig. 2

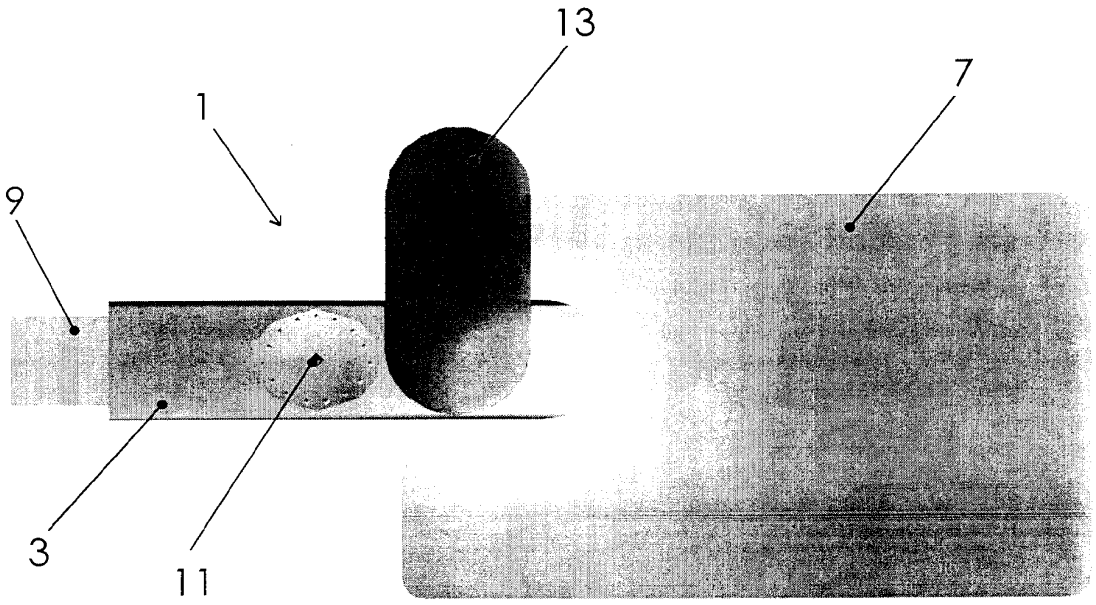


Fig. 3

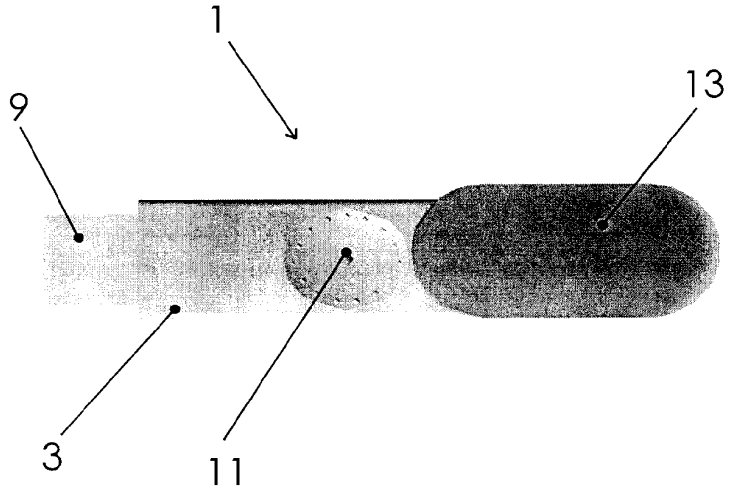


Fig. 4

INTERNATIONAL SEARCH REPORT

Interna al Application No
PCT/IT 00/00429

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06K7/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06K G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 97 07448 A (SIRBU CORNEL) 27 February 1997 (1997-02-27) page 9, line 14 -page 11, line 5 figures 1,7	1-4,6
X	US 5 778 071 A (AMORUSO VICTOR P ET AL) 7 July 1998 (1998-07-07) column 2, line 24 - line 47 column 3, line 6 - line 8 column 6, line 62 -column 7, line 20 figure 1C	1,3,4,6
X	US 5 844 497 A (GRAY ROBERT J) 1 December 1998 (1998-12-01) column 3, line 36 -column 5, line 48 figures 1,2	1,3,4,6

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 January 2001	06/02/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Rydman, J

2

Form PCT/ISA/210 (second sheet) (July 1992)

IPR2022-00412
Apple EX1053 Page 601

INTERNATIONAL SEARCH REPORT

Interna al Application No
PCT/IT 00/00429

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 635 701 A (GLOTON JEAN-PIERRE) 3 June 1997 (1997-06-03) column 2, line 57 -column 3, line 13 figures 1,2 ---	1
A	FR 2 774 194 A (SCM SCHNEIDER MICROSYSTEME MIC) 30 July 1999 (1999-07-30) page 2, line 23 -page 3, line 30 figures 5,7 -----	1

2

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

IPR2022-00412
Apple EX1053 Page 602

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internal Application No
PCT/IT 00/00429

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9707448 A	27-02-1997	FR 2738070 A	28-02-1997
		FR 2740885 A	09-05-1997
		AU 720839 B	15-06-2000
		AU 6824096 A	12-03-1997
		BG 102336 A	30-12-1998
		BR 9610236 A	15-06-1999
		CN 1194043 A	23-09-1998
		CZ 9800408 A	16-12-1998
		EP 0870222 A	14-10-1998
		HU 9900499 A	28-06-1999
		JP 11511278 T	28-09-1999
		NO 980728 A	20-04-1998
		PL 325164 A	06-07-1998
		SK 22098 A	07-10-1998
		US 6070796 A	06-06-2000
US 5778071 A	07-07-1998	US 5546463 A	13-08-1996
		AU 726397 B	09-11-2000
		AU 4147097 A	06-03-1998
		EP 0916210 A	19-05-1999
		WO 9807255 A	19-02-1998
		US 5878142 A	02-03-1999
US 5844497 A	01-12-1998	US 6087955 A	11-07-2000
US 5635701 A	03-06-1997	FR 2716988 A	08-09-1995
		DE 69518678 D	12-10-2000
		EP 0670556 A	06-09-1995
		JP 7271888 A	20-10-1995
FR 2774194 A	30-07-1999	EP 1050006 A	08-11-2000
		WO 9938104 A	29-07-1999

IPR2022-00412
Apple EX1053 Page 603

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
5. Juli 2001 (05.07.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/48339 A1

(51) Internationale Patentklassifikation[7]: E05B 19/04, 49/00

(21) Internationales Aktenzeichen: PCT/EP00/11619

(22) Internationales Anmeldedatum:
22. November 2000 (22.11.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 62 975.7 24. Dezember 1999 (24.12.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **HUF HÜLSBECK & FÜRST GMBH & CO. KG** [DE/DE]; Steeger Strasse 17, 42551 Velbert (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **JACOB, Dirk** [DE/DE]; Breslauer Strasse 13, 42579 Heiligenhaus (DE). **MÜLLER, Ulrich** [DE/DE]; Schneegelskothen 7c, 42549 Velbert (DE). **PLATE, Jeffrey, D.** [US/US]; 9395 North 49th Street, Apt. 201, Brown Deer, WI 53223 (US).

(74) Anwalt: **MENTZEL, Norbert**; Kleiner Werth 34, 42275 Wuppertal (DE).

(81) Bestimmungsstaaten *(national)*: AU, BR, CN, IN, JP, KR, US.

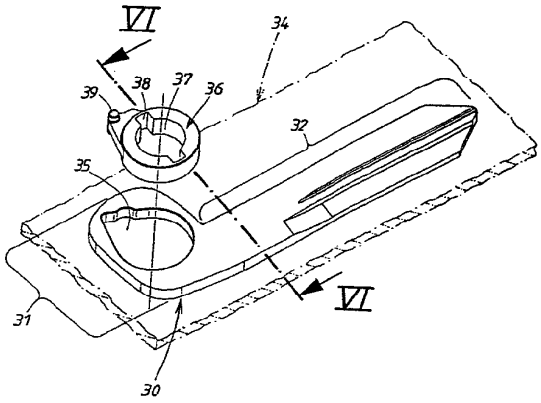
(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Veröffentlicht:
— *Mit internationalem Recherchenbericht.*

[Fortsetzung auf der nächsten Seite]

(54) Title: COMBINED MECHANICAL AND ELECTRONIC KEY, IN PARTICULAR FOR THE LOCKS OF MOTOR VEHICLES

(54) Bezeichnung: KOMBINIERTER MECHANISCHER UND ELEKTRONISCHER SCHLÜSSEL, INSBESONDERE FÜR AN FAHRZEUGEN BEFINDLICHE SCHLÖSSER



(57) Abstract: The invention relates to a combined mechanical and electronic key comprising a key housing for electronic components and an L-shaped flat key (30). Said flat key consists of a bearing limb (31) which enables the key to pivot into a storage position and a shank (32) which mechanically operates the lock. The shank (32) of the flat key (30) can be displaced between an inoperative position, retracted into the key housing and an operative position, in which it projects out of the housing. A push-button preferably also acts as the pivoting axis for the flat key (30). The push-button and the housing have profiled sections and the bearing limb has co-operating profiled sections (37, 38, 39), to subject the flat key (30) to a force in the operative position and to lock the key in one of its positions. The invention aims to produce a simple, cost-effective key. To this end, the flat key is configured as a planar plate (34) with an L-shaped outline, the shank (32) sharing the same plane as the bearing limb. The bearing limb (31) has an opening (35) in the plate for receiving, in a rotationally fixed manner, an insert (36) that has the co-operating profiled section (37 to 39).

[Fortsetzung auf der nächsten Seite]

WO 01/48339 A1

— *Vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen.*

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Bei einem kombinierten mechanischen und elektronischen Schlüssel gibt es sowohl einen Schlüsselbehälter für elektronische Bauteile als auch einen L-förmigen Flachschlüssel (30), der einen zu seiner Schwenklagerung dienenden Lagerschenkel (31) und einen zur mechanischen Betätigung des Schlosses dienenden Schaftschenkel (32) besitzt. Der Flachschlüssel (30) ist mit seinem Schaftschenkel (32) zwischen einer in den Schlüsselbehälter eingeschwenkten Ruhelage und einer herausgeschwenkten Gebrauchslage bewegbar. Ein Druckknopf dient vorzugsweise zugleich als Schwenkachse für den Flachschlüssel (30). Der Druckknopf und der Behälter besitzen Profile und der Lagerschenkel Gegenprofile (37, 38, 39), um den Flachschlüssel (30) in seine Gebrauchslage kraftzubelasten und in einer seiner Lagen zu arretieren. Für eine einfachere und kostengünstigere Herstellung wird vorgeschlagen, den Flachschlüssel als ebene Platte (34) mit L-förmigem Umrissprofil auszubilden, wo der Schaftschenkel (32) in der gleichen Ebene wie der Lagerschenkel angeordnet ist. Dabei besitzt der Lagerschenkel (31) einen Plattendurchbruch (35), der zur drehfesten Aufnahme eines das Gegenprofil (37 bis 39) aufweisenden Einsatzes (36) dient.

Kombinierter mechanischer und elektronischer Schlüssel, insbesondere für an Fahrzeugen befindliche Schlösser

Die Erfindung richtet sich auf einen kombinierten Schlüssel der im Oberbegriff des Anspruches 1 angegebenen Art. Ein solcher Schlüssel erlaubt sowohl eine unmittelbare mechanische Betätigung der Schlösser als auch, alternativ oder ergänzend, eine elektronische Betätigung, z.B. eine Fernbedienung dieses Schlosses bzw. auch anderer Schlösser. Der Schlüsselbehälter ist das Handhabungsmittel sowohl zur mechanischen als auch elektrischen Schlüsselbetätigung. Für die elektronische Betätigung besitzt daher der Schlüsselbehälter an seiner Außenseite Betätigungsstellen, z.B. in Form von elektrischen Druckknöpfen oder nachgiebigen Membranen, die auf im Behälterinneren angeordnete elektrische Schalter od. dgl. einwirken. Der mechanische Flachschlüssel ist L-förmig gestaltet und mit seinem einen L-Schenkel am Vorderende des Behälters schwenkbar gelagert, weshalb der „Lagerschenkel" genannt werden soll. In der Ruhelage befindet sich der Flachschlüssel mit seinem anderen, den Schlüsselschaft bildenden L-Schenkel in einer Einschwenkposition im Behälter. Dieser L-Schenkel soll nachfolgend „Schaftschenkel" bezeichnet werden. Der Flachschlüssel lässt sich mit seinem Schaftschenkel in eine Gebrauchslage herauschwenken. Zur Lagesicherung empfiehlt es sich den Flachschlüssel in beiden Lagen im Schlüsselbehälter zu arretieren.

Bei dem bekannten Schlüssel der im Oberbegriff von Anspruch 1 genannten Art (EP 0 267 429) ist der L-förmige Flachschlüssel mit seinen Schenkeln zweiteilig

IPR2022-00412
Apple EX1053 Page 606

ausgebildet; er besitzt ein Kopfstück in Form eines Lagerrings mit einem tangentialen Ansatz, in welchen das Ende einer Klinge einsteckbar und darin lösbar befestigt ist. Das eingesteckte Kupplungsstück der Klinge muss durch eine Schraube oder einen Niet in der Einstecklage gesichert werden, was mühsam und zeitaufwendig ist. Der den Schaftschenkel bildende L-Schenkel des bekannten Flachschlüssels umfasst den Lagerring, den Ansatz und die eingesteckte Klinge. Der Schaftschenkel ist also zweistückig ausgebildet. Der Übergangsbereich zwischen der eingesteckten Klinge und dem Ansatz am Lagerring ist bruchgefährdet. Um einen Bruch auszuschließen muss das den Aufnahmeschlitz für die Klinge umschließende Material im Ansatz des Lagerrings möglichst dick ausgebildet werden, was der Zielsetzung eines raumsparenden Schlüssels entgegenläuft.

Bei einem bekannten Schlüssel (DE 39 02 537 C2) ist im Schwenkachsenbereich des Flachschlüssels ein mechanischer Druckknopf angeordnet, der axial und radial gefedert ist. Der Druckknopf dient als Schwenkachse für den Flachschlüssel. Die doppelte Federung des Druckknopfes hat zwei Aufgaben beim Flachschlüssel zu erfüllen. Die eine Aufgabe besteht darin, den Flachschlüssel in Schwenkrichtung aus seiner Ruhelage in Richtung seiner Gebrauchslage federzubelasten. Die andere Aufgabe liegt darin, möglichst beide Schwenklagen des Flachschlüssels zu arretieren. Dafür benötigt der Druckknopf geeignete Profilierungen und der Flachschlüssel geeignete Gegenprofilierungen. Zwar ist der Flachschlüssel L-förmig ausgebildet, doch muss der Lagerschenkel wegen der Gegenprofile eine beachtliche Bauhöhe aufweisen und wird gesondert als Lagerkörper mit Vierkantprofil vorgefertigt. Um die große Bauhöhe des Lagerkörpers zu nutzen, ordnete man den Schaftschenkel in einer Parallelebene zur Schwenkachse des Flachschlüssels an. Das erfordert eine entsprechend große Höhendimension im Schlüsselbehälter. Der zur Lagerung des mechanischen Druckknopfs dienende Lagerkörper des Flachschlüssels besitzt einen Schlitz zur nachträglichen Anbringung des für sich gefertigten Schlüsselschafts. Der Schlüsselschaft wird in den Schlitz des Lagerkörpers eingesteckt und dort durch einen Stift od. dgl. gesichert. Das ist zeit- und kostenaufwendig.

Es gibt kombinierte Schlüssel (DE 22 26 385 A; DE 38 42 790 C1), die zwar einen flachen L-förmigen Flachschlüssel aufweisen, doch ist ein Druckknopf im

IPR2022-00412
Apple EX1053 Page 607

Achsbereich nicht vorgesehen. Die Schwenkachse erzeugt ein unbeweglicher Lagerstift. Weil kein Gegenprofil für einen Druckknopf erforderlich ist, kann der zur Schwenklagerung dienende eine Lagerschenkel des Flachprofils flach ausgebildet sein. Man bildet den Flachschlüssel als eine ebene Platte aus, in welcher auch das Flachprofil des Schaftschenkels liegt. Dieses Schlüsselgehäuse kann zwar flacher gebaut werden, doch gibt es keine Federbelastung, um den Schaftschenkel aus einer in dem Schlüsselbehälter abgesenkten Ruhelage in seine herausgeschwenkte Gebrauchslage zu überführen. Dies erfordert eine mühsame Handhabung. Außerdem gibt es keine raumsparende Möglichkeit, um den Flachschlüssel in diesen Lagen im Behälter zu arretieren. Diese nicht festlegbare Schwenkposition des Flachschlüssels bringt Probleme sowohl beim Tragen in der Hosentasche als auch beim Gebrauch, z.B. während der Drehbetätigung des Schlüsselgehäuses.

Bei Schraubverbindungen an Blechprofilen ist es bekannt, zum Erreichen der nötigen Einschraublänge für die Schraube das Mutterngewinde im Blechprofil durch ein Ansatzstück oder ein eingenietetes Einsatzstück zu vergrößern (U. Richter, R. v. Voss, F. Kozer: Bauelemente der Feinmechanik, Berlin: Verlag Technik, 1954, S. 137). Diese Ausbildung von Mutterngewinden in Blechprofilen steht mit Flachschlüsseln in keinem Zusammenhang. Diese Druckschrift gibt keine Anregungen für den Aufbau eines L-förmigen Flachschlüssels.

Der Erfindung liegt die Aufgabe zugrunde, einen zuverlässigen, raumsparenden Schlüssel der im Oberbegriff des Anspruches 1 genannten Art zu entwickeln, der sich einfacherer und kostengünstiger herstellen lässt. Dies wird erfindungsgemäß durch die im Kennzeichen des Anspruches 1 angeführten Maßnahmen erreicht, denen folgende besondere Bedeutung zukommt.

Bei der Erfindung wird zunächst der Schlüssel mit seinen beiden L-Schenkeln einstückig in Form einer ebenen Platte ausgebildet. Man kann den L-förmigen Flachschlüssel aus Plattenmaterial ausstanzen. Durch die einstückige Ausbildung liegt ein stabiler bruchfester Übergang zwischen dem Lagerschenkel und dem Schaftschenkel vor. Trotz der flachen Ausbildung dieses L-förmigen Schlüssels kann im Bereich seines Lagerschenkels der mechanische Druckknopf im Schlüsselbehälter

IPR2022-00412
Apple EX1053 Page 608

eingesetzt werden. Dies ist deswegen möglich, weil die für den Druckknopf an sich erforderlichen Gegenprofile einem Einsatz überlassen werden, der in einem Plattendurchbruch des Lagerschenkels drehfest aufgenommen wird. Der Einsatz dient sowohl zur Schwenklagerung als auch zweckmäßigerweise zur Axialführung des Druckknopfs und zur Aufnahme seiner Federmittel. Dadurch ist auch der Aufbau des Schlüsselbehälters vereinfacht. Trotz einer einstückigen, preiswerten L-Plattenform des Flachschlüssels lässt sich seine Arretierung in der Ruhe- und Gebrauchslage über den Druckknopf zuverlässig verwirklichen. Außerdem wird der Schlüssel durch die am Druckknopf und Einsatz vorgesehenen Mitnahmeflächen mittels der auf ihn wirkende Federkraft aus einer Ruhelage in die Gebrauchslage selbsttätig herausgeschwenkt, wenn in der Ruhelage die Arretierung durch Betätigen des Druckknopfs unwirksam gesetzt worden ist.

Weitere Maßnahmen und Vorteile der Erfindung ergeben sich aus den Unteransprüchen, der nachfolgenden Beschreibung und den Zeichnungen. In den Zeichnungen ist die Erfindung in einem Ausführungsbeispiel schematisch dargestellt. Es zeigen:

Fig. 1, in perspektivischer Darstellung, den Schlüsselbehälter mit herausragendem mechanischen Flachschlüssel,

Fig. 2, ebenfalls in perspektivischer Darstellung, eine zum Flachschlüssel von Fig. 1 gehörende Steckeinheit, bestehend aus einer die elektronischen Bauteile umschließenden Elektrokapsel,

Fig. 3 ein aus dem Schlüsselbehälter von Fig. 1 und der Steckeinheit von Fig. 2 zusammengestecktes Kombinationsgehäuse, das zur Handhabung bei mechanischer und elektronischer Betätigung des Schlüssels dient,

Fig. 4, in Explosionsdarstellung, einige wesentliche Bestandteile des in Fig. 1 gezeigten Schlüsselbehälters mit dem mechanischen Flachschlüssel, vor deren Zusammenbau,

IPR2022-00412
Apple EX1053 Page 609

Fig. 5, in Explosionsdarstellung, die beiden Bestandteile des mechanischen Flachschlüssels vor ihrer Vereinigung,

Fig. 6 einen Querschnitt durch den einen Bestandteil von Fig. 5, längs der dortigen Schnittlinie VI - VI,

Fig. 7 einen Querschnitt durch das zusammengebaute Schlüsselbehälter von Fig. 1 längs der dortigen Schnittlinie VII - VII, wobei ein Druckknopf in seiner eingedrückten Position gezeigt ist,

Fig. 8 einen Axialschnitt durch den in Fig. 1 gezeigten Schlüsselbehälter längs der dortigen Schnittlinie VIII - VIII und

Fig. 9 einen Querschnitt durch das in Fig. 3 gezeigte Kombinationsgehäuse längs der dortigen Schnittlinie IX - IX.

Der kombinierte Schlüssel nach der Erfindung erlaubt sowohl eine mechanische als auch eine elektronische Betätigung eines nicht näher gezeigten Schlosses. Er besteht aus zwei jeweils für sich vorgefertigten Teilen 10, 20, die nachträglich ineinandergefügt werden. Der eine Teil 10 umfasst die mechanischen Schließmittel und besteht aus einem Schlüsselbehälter 10, dessen Bestandteile aus der Explosionsdarstellung von Fig. 4 am besten zu erkennen sind. Der andere Teil 20 ist eine noch näher zu beschreibende Steckeinheit, welche die in ihrem Inneren die im Querschnitt von Fig. 9 angedeuteten elektronischen Bauteile 40 umfasst.

Ausweislich der Fig. 1 und 4 umfasst der mechanische Teil zunächst einen zweischaligen Schlüsselbehälter 10. Während die Oberschale 11, wie Fig. 7 und 8 erkennen lässt, als ebene Platte mit stellenweisen Kupplungsvorsprüngen 13 an ihrer Innenfläche ausgebildet ist, umfasst die Unterschale 12 außer ihrem Schalenboden 15 auch noch Schalenseitenwände 14. In den Schalenseitenwänden 14 befinden sich stellenweise Kupplungsaufnahmen 16 für die vorerwähnten Kupplungsvorsprünge 13 der Oberschale 11. Die Oberschale 11 erstreckt sich nur über einen vorderen Bereich

des Schlüsselbehälters 10 und weist im hinteren Bereich einen Ausbruch 17 auf, der zum Schaleninneren 18 hin einen von außen zugänglichen Freiraum erzeugt. Das ist für das noch näher zu beschreibende Einstecken bzw. Herausziehen der Steckeinheit 20 bedeutungsvoll.

Zum Schlüsselbehälter 10 gehört, wie Fig. 4 zeigt, ein mechanischer Flachschlüssel 30 der beweglich angeordnet ist, um aus einer nicht näher gezeigten versenkten Ruhelage im Behälter 10 in eine aus dem Behälter herausragenden, in Fig. 1 bis 4 ersichtliche Gebrauchslage überführt zu werden. Der Flachschlüssel 30 besteht aus metallischem Werkstoff. Obwohl auch andere Bewegungen denkbar wären, ist dieser Flachschlüssel 30 um die strichpunktiert in den Fig. 1, 3 und 4 angedeuteten Schwenkachsen 33 schwenkbeweglich. Dabei ist der Flachschlüssel 30 als ein Stanzling aus einer in Fig. 4 strichpunktiert verdeutlichten ebenen Platte 34 ausgebildet, wobei der Stanzling ein L-förmiges Umrissprofil aus zwei Schenkeln 31, 32 besitzt. Der eine L-Schenkel ist kurz ausgebildet und dient zur Schwenklagerung des Flachschlüssels 30 am Vorderende des Schlüsselbehälters 10 und wird daher nachfolgend kurz „Lagerschenkel" genannt. Der andere L-Schenkel 32 umfasst das eigentliche Flachprofil des Schlüsselschafts, weshalb er nachfolgend als „Schaftschenkel" bezeichnet werden soll. Beide Schenkel 31, 32 liegen also in einer gemeinsamen, durch den erwähnten Plattenverlauf 34 bestimmten Ebene, die im fertig montierten Zustand des Schlüsselbehälters 10 senkrecht zur Schwenkachse 33 verläuft. Ausweislich der Fig. 5 ist der Lagerschenkel 31 mit einem unrunden Plattendurchbruch 35 versehen, der zur Aufnahme eines besonderen Einsatzes 36 dient.

Der Druckknopf 40 ist sowohl axial als auch radial federbelastet und besitzt mit dem Behälter 10 übereinstimmend ausgebildete Profile 19, 48, 28. Der Einsatz 36 besteht aus relativ nachgiebigem Material, vorzugsweise Kunststoff und besitzt ein besonderes Gegenprofil 37, 38, 39 für einen die Lage der Schwenkachse 33 bestimmenden Druckknopf 40. Die Federwirkung übernimmt eine kombinierte Druck-Dreh-Feder 41, die, ausweislich der Fig. 7, in einer Axialbohrung 45 des Druckknopfs 40 aufgenommen ist. Die Feder 41 ist mit ihrem einen Federende 42 drehfest mit dem Druckknopf 40 verbunden, während ihr anderes Federende 43 in der

IPR2022-00412
Apple EX1053 Page 611

Unterschale 12 des Behälters 10 festgehalten wird. Die Feder 41 ist wendelförmig ausgebildet. Im Montagefall greift ein an der bodenseitigen Innenfläche der Unterschale 12 sitzender Dorn 44 sowohl ins Wendelinnere hinein, als auch in den Einsatz 36 ein.

Gemäß Fig. 5 wird zunächst der Flachschlüssel 30 mit seinem Plattendurchbruch 35 durch Stanzen erzeugt und dann, nachträglich, der Einsatz 36 in den Plattendurchbruch 35 vertikal eingesteckt. Nach diesem Einstecken ragt, wie Fig. 4 und 7 zeigen, über die beiden Plattenflächen des Flachschlüssels heraus. Dazu gehören zylindrische Ansätze 47, gemäß Fig. 6, aber auch ein Anschlagzapfen 39 an beiden Flächenseiten, der in ein Ringnutsegment 19 der beiden Schalen 11 und 12 hineinragt, wie aus Fig. 8 zu entnehmen ist. In der in Fig. 8 ausgezogen gezeichneten Position des Anschlagnockens 39 liegt die bereits eingangs erwähnte, aus dem Behälter 10 herausgeschwenkte Gebrauchslage vor. Dann erstreckt sich der vorbeschriebene Schaftschenkel 32 des Flachschlüssels 30 in Richtung der in Fig. 8 strichpunktiert angedeuteten Hilfslinie 30.1, welche die in den übrigen Fig. dargestellte Gebrauchslage des Flachschlüssels 30 kennzeichnet. In dieser Gebrauchslage 30.1 ist der Flachschlüssel durch den Druckknopf 40 arretiert. Dann greifen am Druckknopf 40 vorgesehene, hier diametral angeordnete Mitnahmeflügel 48 in zugehörige Radialnuten 28 an der Innenfläche der Oberschale 11 hinein und sichern so die Ausschwenklage des Flachschlüssels 30.

Die Mitnahmeflügel 48 besitzen, als Gegenprofil, im Einsatz 36 Axialnuten 48, die eine Eindruckbewegung im Sinne des aus Fig. 7 erkennbaren Kraftpfeils 46 zulassen. Diese Eindruckbewegung 46, die in Fig. 7 vollzogen ist, führt zu einer axialen Absenkung des Druckknopfs 40, wodurch die Mitnahmeflügel 48 die Radialnuten 28 freigeben. Die Eindruckbewegung 46 erfolgt gegen die axiale Kraftwirkung der Feder 41. Die Arretierung der Gebrauchslage 30.1 ist dann aufgehoben. Der Flachschlüssel kann dann im Sinne des Bewegungspfeils 29 von Fig. 8 gegen die durch den Kraftpfeil 49 in Fig. 8 verdeutlichte Drehkraft der Feder 41 in seine Ruhelage im Gehäuse zurückgeschwenkt werden. Dann liegt der Schaftschenkel 32 des Flachschlüssels 30, in Fig. 8 gesehen, an der dort mit 30.2 gekennzeichneten Strichpunktlinie. In dieser Ruhelage 30.2 verschwindet der Schaftschenkel 32 in

einem aus Fig. 3 erkennbaren seitlichen Spalt 24 eines noch näher zu beschreibenden Gesamtgehäuses 50, welches aus dem Schlüsselbehälter 10 und der darin eingeschobenen Steckeinheit 20 entsteht. Dann sind die Mitnahmeflügel 48 wieder in axialer Ausrichtung mit den gehäuseseitigen Radialnuten 28, wo sie durch die Rückstellkraft der Feder 41 einschnappen und so auch diese Ruhelage 30.2 des Flachschlüssels 30 im Schlüsselbehälter 10 arretieren.

Bei der Schwenkbewegung 29 dient der Druckknopf 40 auch als Schwenklager. Dazu ist in der Oberschale 11 des Behälters 10 eine aus Fig. 4 erkennbare Lagerbohrung 25 vorgesehen. Diese ist in axialer Ausrichtung mit einer in Fig. 5 und 6 gezeigten Axialbohrung 37 des Einsatzes 36 und mit dem bereits mehrfach erwähnten Dorn 44 der Unterschale 12. Der Druckknopf 40 bestimmt die Schwenkachse 33 des Flachschlüssels 30. Der Anschlagzapfen 39 vom Einsatz 36 einerseits und das ihm gehäuseseitig zugeordnete Ringnutsegment 19 andererseits können auch Drehführungsfunktionen bei der Schwenkbewegung 29 übernehmen. Außerdem können Drehanschläge durch das Umrissprofil des Schlüssels 30 einerseits und Innenflächen an den beiden Schalen 11, 12 andererseits verwirklicht sein.

Statt einer Vorfertigung des Einsatzes 36 könnte man den Einsatz 36 durch eine Spritzgusstechnik nachfertigen. Dazu wird der beschriebene Flachschlüssel 30 in eine Spritzgussform eingebracht, in welcher dann der Einsatz 36 im Plattendurchbruch 35 durch Gießen gebildet wird. Die erwähnte Gegenprofilierung 37, 38, 39, 47 liegt dann in ähnlicher Form vor.

In manchen Anwendungsfällen ist bei dem eingangs erwähnten kombinierten Schlüssel für die elektronische Betätigung auch ein sogenannter Transponder 26 erwünscht. Dieser Transponder 26 soll bereits zur elektronischen Individualisierung dieses kombinierten Schlüssels sorgen. Wird dieser Schlüssel in das zugehörige Schloss eingesteckt, so findet zwischen dem Transponder 26 und dem Schloss eine Kommunikation statt, die bei Übereinstimmung von Schloss und Schlüssel bereits Schlossfunktionen auslöst. Deswegen werden bei der Erfindung derartige Transponder 26 im vorderen Bereich des Schlüsselbehälters 10 untergebracht. Dazu besitzt die Unterschale 12 eine Kammer 27, in welche der bzw. die Transponder 26

eingeklebt werden können. Weil eine elektronische Energieversorgung der Transponder 26 nicht erforderlich ist, braucht der fertig montierte Schlüsselbehälter 10 von Fig. 1 nicht mehr in seine Schalen 11, 12 zerlegt zu werden, um dort einen Batteriewechsel od. dgl. vorzunehmen. Die Transponder 26 sind also in der Kammer 27 permanent geschützt. Das gilt auch für die bereits eingangs erwähnten weiteren elektronischen Bauteile 21, welche innerer Bestandteil der bereits erwähnten lösbaren Steckeinheit 20 des Gesamtgehäuses 50 sind.

Wie am besten aus Fig. 9 zu ersehen ist, gehören zur Steckeinheit 20 eine gehäuseartige Kapsel 22, in deren Innenraum 23 die Bauteile 21 angeordnet und so nach außen allseitig abgeschlossen sind. Im Kapselinneren 23 können auch die Schaltungen der Bauelemente und gegebenenfalls die elektrische Störung angeordnet sein. Diese Baueinheit 21, 22, die als Steckeinheit mit dem Schlüsselbehälter 10 fungiert, wird komplett vorgefertigt und soll nachfolgend „Elektrokapsel" genannt werden. Dazu ist der Schlüsselbehälter 10 profilmäßig in folgender Weise angepasst.

Der eingangs erwähnte Ausbruch 17 im Schlüsselbehälter 10 erfolgt einfach dadurch, dass die Oberschale 11, gemäß Fig. 1, nur den Vorderabschnitt 51 des Schlüsselbehälters 10 überdeckt. Dadurch ist ein von außen zugänglicher Freiraum ins Schaleninnere 18 erzeugt. Dieser Freiraum 17 besitzt nicht nur eine nach oben weisende Oberöffnung 52, sondern erstreckt sich auch in eine vom Hinterende 54 zugängliche Seitenöffnung 53. Diese entsteht, weil nicht nur der hintere Abschnitt der Oberschale 11 fehlt, sondern auch, wie Fig. 1 zeigt, die Seitenwand 14 der Unterschale 12 am Hinterende 54 des Behälters 10 weggefallen ist. Die Elektrokapsel 20 wird durch diese Seitenöffnung 53 in den Freiraum 17 des Schlüsselbehälters 10 gemäß dem Bewegungspfeil 55 von Fig. 1 eingeschoben. In ihrer Einschublage, gemäß Fig. 3, verschließt die Elektrokapsel 20 die Oberöffnung 52. Die Einschubbewegung 55 ist in einer Parallelebene zu der oben erwähnten Schwenkbewegung 29 angeordnet. Dabei sind folgende Führungsmittel 61, 62 zum gezielten Einstecken und Verschieben 55 der Elektrokapsel 20 vorgesehen.

An der Innenfläche des Schalenbodens 15 der Unterschale 12 befinden sich zwei parallele Führungsleisten 61, die zur Seitenöffnung 53 hin gerichtet sind. Sie sind

IPR2022-00412
Apple EX1053 Page 614

hinterschnitten und besitzen vorzugsweise ein schwalbenschwanzförmiges Profil. Ihnen sind angepasste Führungsnuten 62 an der Unterseite des Gehäuses der Elektrokapsel 20 zugeordnet. Die Eingriffslage dieser Führungsmittel 61, 62 ist im Schnitt von Fig. 9 zu erkennen. Dabei ist die eine Längsseite vom Kapselgehäuse 22 gemäß Fig. 9 bei 58 gestuft, so dass mit einer entsprechenden Stufung 59 in der Unterschale 12, gemäß Fig. 4, in der Einschublage der seitliche Spalt 24 für den Schaftschenkel 32 des Flachschlüssels 30 entsteht. In der Einschublage gemäß Fig. 3 und 9 gehen die sichtbar bleibenden Außenflächen der Elektrokapsel 20 einerseits und des Schlüsselbehälters 10 andererseits ineinander bündig über. Beide Teile 10, 20 bilden dann das bereits erwähnte Kombinationsgehäuse 50, welches beim Handhaben des Schlüssels mit der Hand gemeinsam umgriffen wird und daher „Kombinationsgehäuse" genannt werden soll. Dies gilt sowohl bei einer mechanischen Betätigung des zugehörigen Schlosses, wo der herausgeschwenkte Schaftschenkel 32 mittels des Kombigehäuses 50 gedreht wird, als auch bei der elektronischen Betätigung. Dafür sind Betätigungsstellen 60 an die sichtbar bleibende Außenfläche der Elektrokapsel 20 im gemeinsamen Kombinationsgehäuse 50 vorgesehen. Diese können aus Druckschaltern oder membranartigen Betätigungsstellen entstehen. Diese Betätigungsstellen können mit weiteren membranartigen Überdeckungen im Bereich des vorerwähnten Druckknopfs 40 vorgesehen sein, dem noch folgende besondere Bedeutung zukommt.

Die in Fig. 3 und 9 gezeigte Einstecklage der Elektrokapsel 20 im Schlüsselbehälter 10 ist nicht nur durch Anschlagmittel begrenzt, sondern auch durch Rastmittel gesichert. Diese Funktion kann in vorteilhafterweise auch vom Druckknopf 40 übernommen werden. Dazu ist die Elektrokapsel 20, gemäß Fig. 2, vorderendig mit einem Lappen 56 verlängert, der in der Einschublage von Fig. 3 den verbliebenen Vorderabschnitt 51 der Oberschale 11 vom Schlüsselbehälter 10 überdeckt. Der Lappen 56 besitzt eine Ausnehmung 57, in welche der axial federnde Druckknopf 40 in der Einschublage der Elektrokapsel 20 gemäß Fig. 3 einschnappt. Dadurch ist der Zusammenhalt des Schlüsselbehälters mit der Elektrokapsel 20 sichergestellt. Die Ausnehmung 57 durchsetzt den Lappen 56, weshalb im Eingriffsfall gemäß Fig. 3 der Druckknopf 40 mit einem zu seiner Betätigung ausreichenden Längenstück aus dem Lappen 56 herausragt. Zur Demontage des Kombinationsgehäuses 50 in seine

IPR2022-00412
Apple EX1053 Page 615

Bestandteile 10, 20 wird der Druckknopf 40, wie Fig. 7 zeigt, soweit im Sinne des Pfeils 46 eingedrückt, dass er die Ausnehmung 57 im Lappen 56 freigibt.

Der Druckknopf 40 kann durch eine Membran im Bereich des Lappens 56 überdeckt sein, welche in ähnlicher Weise wie die Betätigungsstellen 61 fungiert. Diese Membrane dieser Betätigungsstellen 61 können mit der vorgenannten Membran im Bereich des Druckknopfs 40 kombiniert sein.

IPR2022-00412
Apple EX1053 Page 616

Bezugszeichenliste :

10	erster Schlüsselteil, Schlüsselbehälter
11	Oberschale von 10
12	Unterschale von 10
13	Kupplungsvorsprung an 11
14	Schalenseitenwand von 12
15	Schalenboden von 12
16	Kupplungsaufnahme von 12
17	Ausbruch von 11, Freiraum in 18
18	Schaleninneres
19	Profil in 11, 12 für 39, Ringnutsegment
20	zweiter Schlüsselteil, Steckeinheit, Elektrokapsel
21	elektronischer Bauteil
22	gehäuseartige Kapsel für 21
23	Kapselinneres für 22 in 21
24	seitlicher Spalt in 50 für 32 (Fig. 3, 9)
25	Lagerbohrung in 11 für 40 (Fig. 4)
26	Transponder
27	Kammer in 11 für 26 (Fig. 4)
28	Profil in 11 für 48 von 40, Radialnut (Fig. 7)
29	Schwenkbewegungspfeil für 30 (Fig. 8)
30	mechanischer Flachschlüssel für 10, Stanzling
30.1	Gebrauchslage von 32 (Fig. 8)
30.2	Ruhelage von 32 (Fig. 8)
31	erster L-Schenkel von 30, Lagerschenkel
32	zweiter L-Schenkel von 30, Schaftschenkel
33	Schwenkachse für 30
34	ebene Platte für 30
35	Plattendurchbruch
36	Einsatz in 35
37	Gegenprofil in 36, Axialbohrung (Fig. 5, 6)

IPR2022-00412
Apple EX1053 Page 617

38 Gegenprofil von 36, Axialnut in 36 für 48 (Fig. 5, 8)
39 Gegenprofil von 36, Führungs- bzw. Anschlagzapfen (Fig. 5, 6)
40 Druckknopf
41 Druck-Dreh-Feder von 40
42 erstes Federende von 41 (Fig. 7)
43 zweites Federende von 41 (Fig. 7)
44 Dorn an 12 für 41 (Fig. 4)
45 Axialbohrung in 40 für 41
46 Pfeil der Eindruckbewegung von 40 (Fig. 7)
47 Gegenprofil an 36, zylindrischer Ansatz an 36 (Fig. 5)
48 Profil, Mitnahmeflügel an 40
49 Pfeil der Ausschwenkkraft von 41 für 30 (Fig. 8)
50 Gesamtgehäuse aus 10, 20, Kombinationsgehäuse
51 Vorderabschnitt von 10
52 Oberöffnung von 10 bei 17 (Fig. 1)
53 Seitenöffnung von 11 (Fig. 1)
54 Hinterende von 10
55 Pfeil der Einschubbewegung von 20 in 10 (Fig. 1)
56 Lappen an 20 (Fig. 2)
57 Ausnehmung in 56 für 40 (Fig. 2)
58 Innenstufung von 22 für 24 (Fig. 2, 9)
59 Stufe von 12 für 24 (Fig. 4)
60 Betätigungsstelle an 20 (Fig. 1)
61 Führungsmittel an 12, Führungsleiste
62 Führungsmittel an 20, Führungsnut

Patentansprüche :

1.) Kombinierter mechanischer und elektronischer Schlüssel, insbesondere für in Fahrzeugen befindliche Schlösser,

mit einem gemeinsamen, bei der Schlüsselbetätigung zu handhabenden Schlüsselbehälter (10) sowohl für elektronische Bauteile (21) zur elektronischen Betätigung des Schlosses als auch für einen L-förmigen Flachschlüssel (30) zur mechanischen Betätigung des Schlosses,

wobei der Flachschlüssel (30) mit seinem einen L-Schenkel, dem Lagerschenkel (31), am Vorderende (51) des Behälters (10) schwenkgelagert (33) ist,

wobei sein anderer, den eigentlichen Schlüsselschaft mit Flachprofil bildender L-Schenkel, der Schaftschenkel (32), aus einer im Behälter (10) eingeschwenkten Ruhelage (30.2) in eine herausgeschwenkte Gebrauchslage (30.1) bewegbar ist,

mit einer axial und radial wirksamen Federbelastung (41)

und mit einem Druckknopf (40), der vorzugsweise zugleich die Schwenkachse (33) des Flachschlüssels (30) im Schlüsselbehälter (10) bestimmt,

wobei der Druckknopf (40) und der Behälter (10) Profile (48, 28) aufweisen und der Lagerschenkel (31) Gegenprofile (37, 38, 39, 47) besitzt, durch die der Flachschlüssel (30) einerseits in seine Gebrauchslage (30.1) kraftbelastet und andererseits in wenigstens einer seiner Lagen (30.1; 30.2) arretiert wird,

und der Schaftschenkel (32) in der gleichen, senkrecht zur Schwenkachse (33) verlaufenden Ebene angeordnet ist, wie der mit dem Druckknopf (44) zusammenwirkende Lagerschenkel (31),

IPR2022-00412
Apple EX1053 Page 619

dadurch gekennzeichnet,

dass der L-förmige Flachschlüssel (30) mit seinen beiden Schenkelenden (31, 32) als einstückige ebene Platte ausgebildet ist,

dass der Lagerschenkel (31) einen unrunden Plattendurchbruch (35) besitzt

und dass der Plattendurchbruch (35) zur drehfesten Aufnahme eines Einsatzes (36) dient, der ein Gegenprofil (37, 38, 39, 47) aufweist.

2.) Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass der L-förmige Flachschlüssel (30) und sein unrunder Plattendurchbruch (35) durch Stanzen aus dem Plattenmaterial (34) erzeugt sind und einen Stanzling bildet.

3.) Schlüssel nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass der Einsatz (36) mit seinem Gegenprofil (37, 38, 39, 47) als Vorprodukt herstellbar ist und einen unrunden Umriss aufweist,

und dass der Einsatz (36) nachträglich in den Plattendurchbruch (35) eingesteckt und dort kraft- und/oder formschlüssig festgehalten ist.

4.) Schlüssel nach einem oder mehreren der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass der Flachschlüssel (30) aus einem relativ formfesten, metallischen Material gebildet ist und der Einsatz (36) aus relativ nachgiebigem Material, vorzugsweise Kunststoff besteht.

5.) Schlüssel nach einem oder mehreren der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass der Einsatz (36) mindestens eine der beiden Plattenflächen des Flachschlüssels (30) wenigstens bereichsweise überragt.

6.) Schlüssel nach Anspruch 1, 2 oder 4, dadurch gekennzeichnet, dass der Einsatz (36) im Bereich des Plattendurchbruchs (35) durch Spritzgusstechnik angeformt und mit dem Flachschlüssel (30) spritzgusstechnisch verbunden ist.

7.) Schlüssel nach einem oder mehreren der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass das Gegenprofil vom Einsatz (36) ein axial abragendes Drehanschlag- und/oder Drehführungs-Element (39) aufweist

und dass das Drehanschlag- und/oder Drehführungs-Element im Montagefall in ein Ringnut-Segment (19) an der Innenfläche des Schlüsselgehäuses (10) hineinragt.

8.) Schlüssel nach einem oder mehreren der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass das Gegenprofil des Einsatzes (36) eine Axialbohrung (37) mit wenigstens einer davon radial abragenden Axialnut (38) umfasst, in welche der Druckknopf (40) mit mindestens einem abgesetzten Mitnahmeflügel (48) zeitweise und/oder bereichsweise eingreift.

IPR2022-00412
Apple EX1053 Page 621

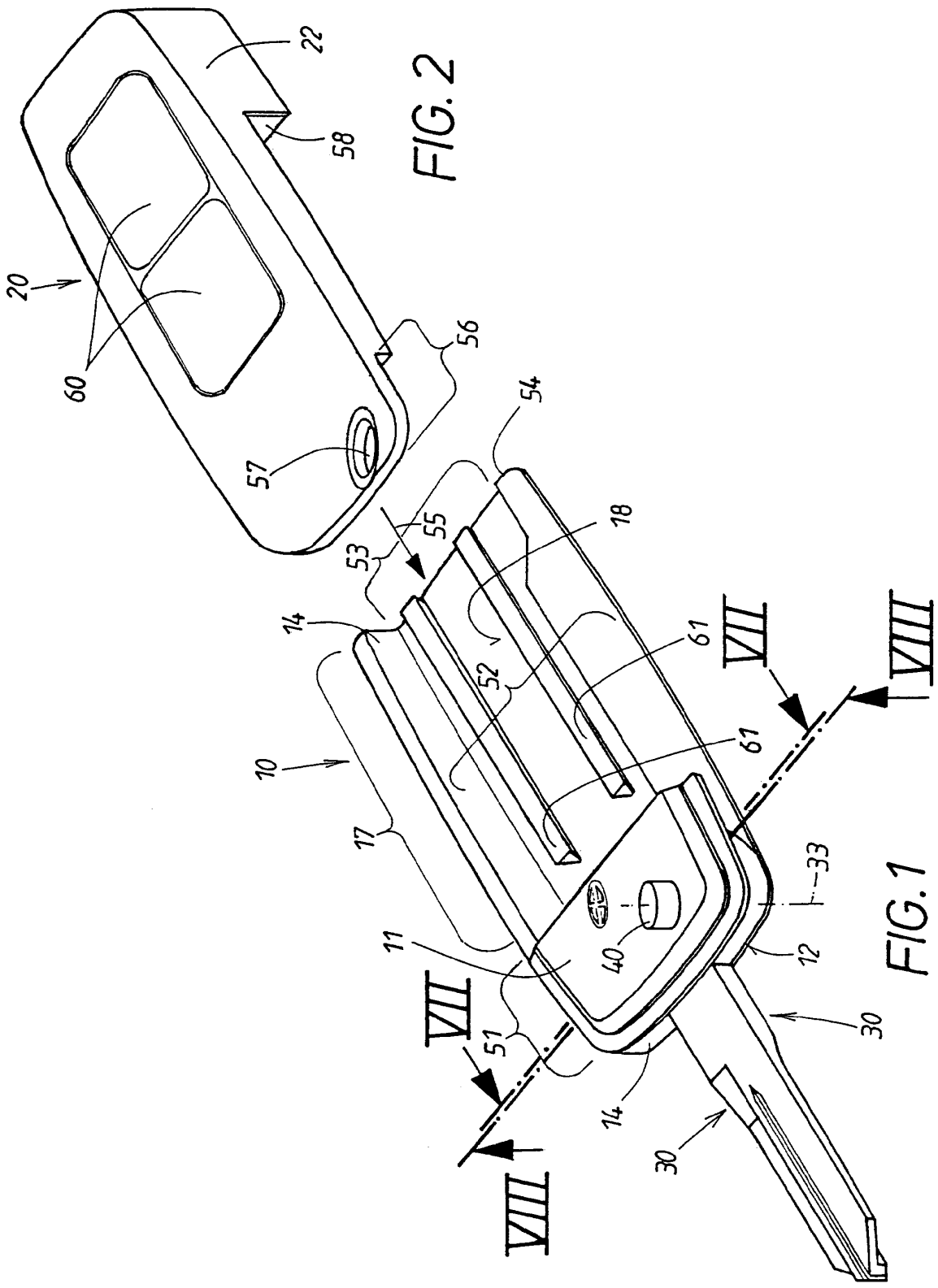

22
58
20
60
56
57
54
55
53
18
14
61
52
VII
VIII
10
17
11
40
33
12
51
30
14
30

FIG. 2

FIG. 1

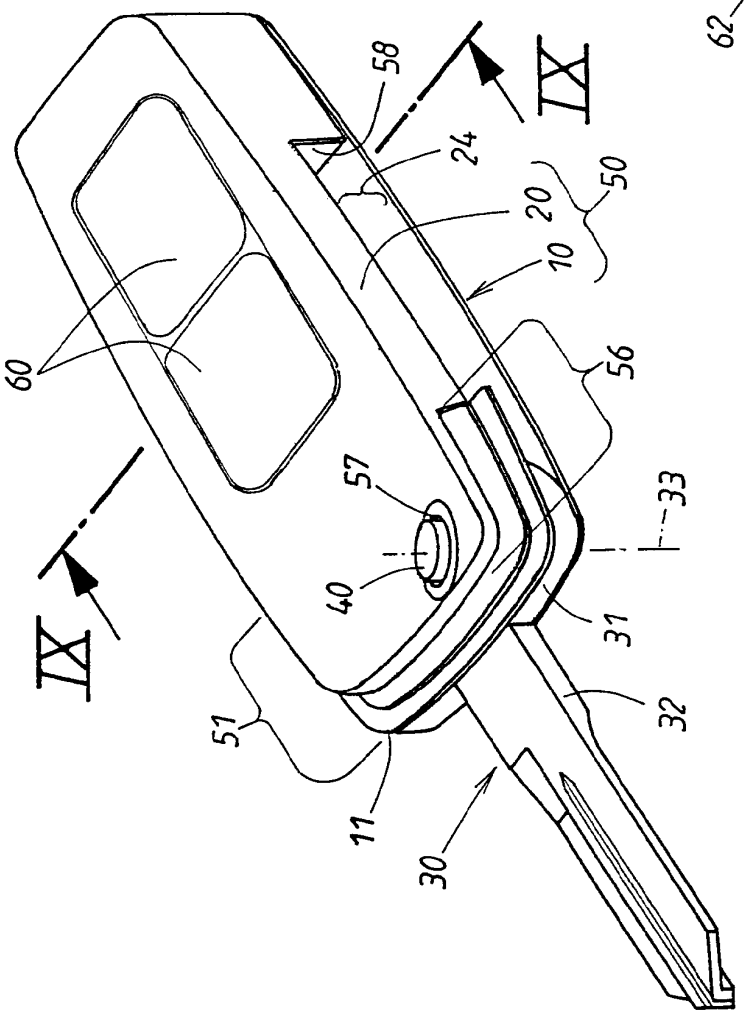

IX
IX
58
24
20
50
10
60
56
57
33
40
31
51
32
11
30

FIG. 3

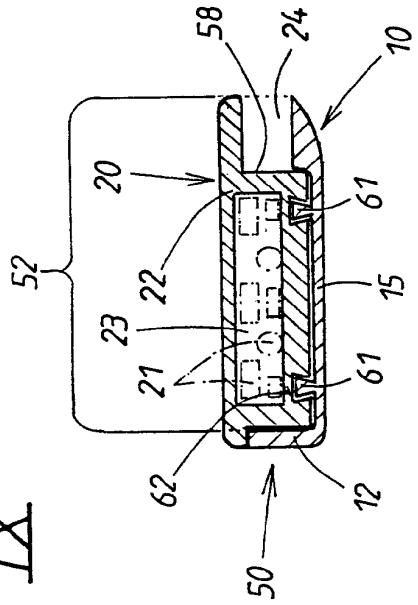

58
24
10
20
61
52
22
15
23
21
61
62
12
50

FIG. 9

315

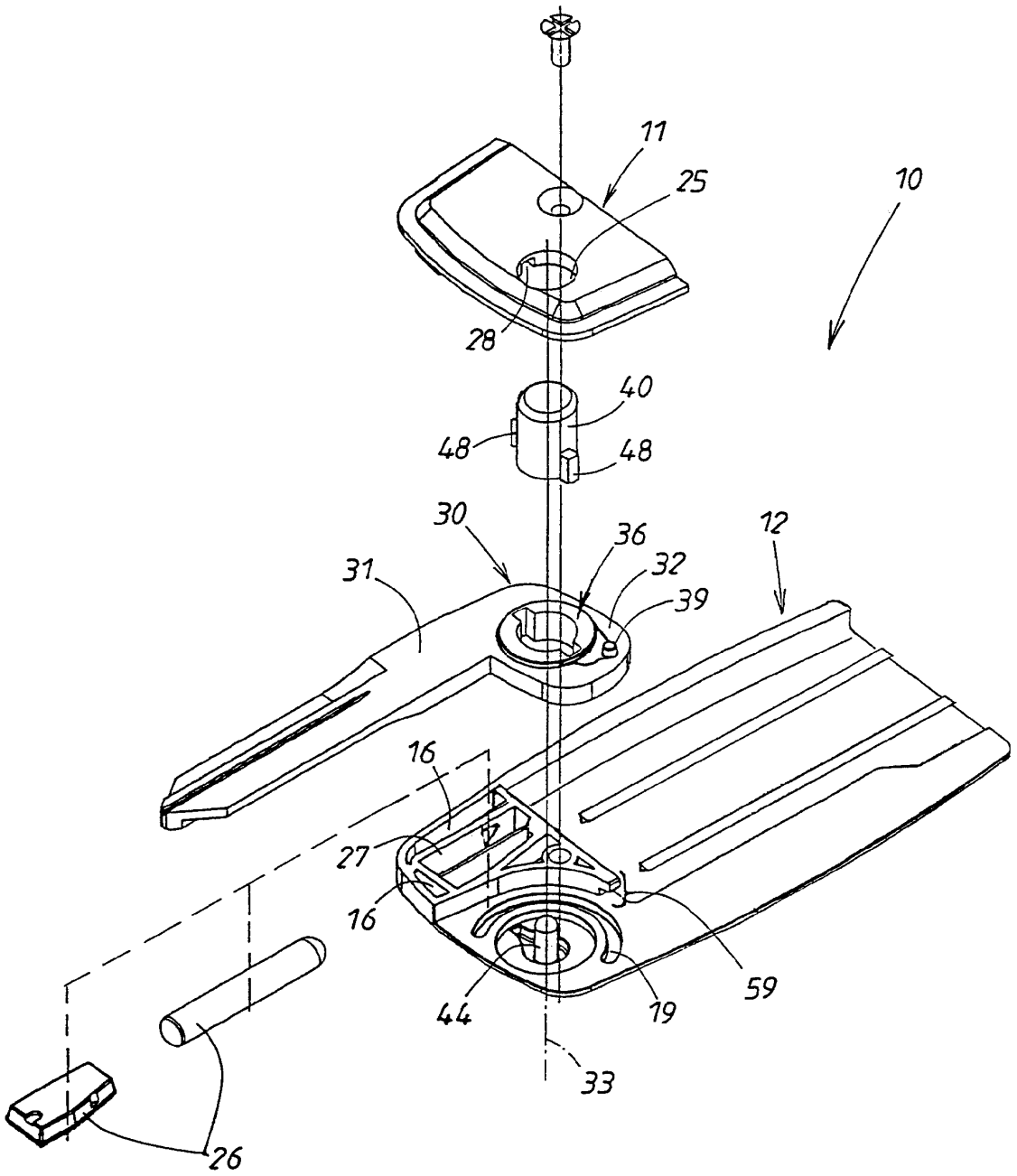


FIG. 4

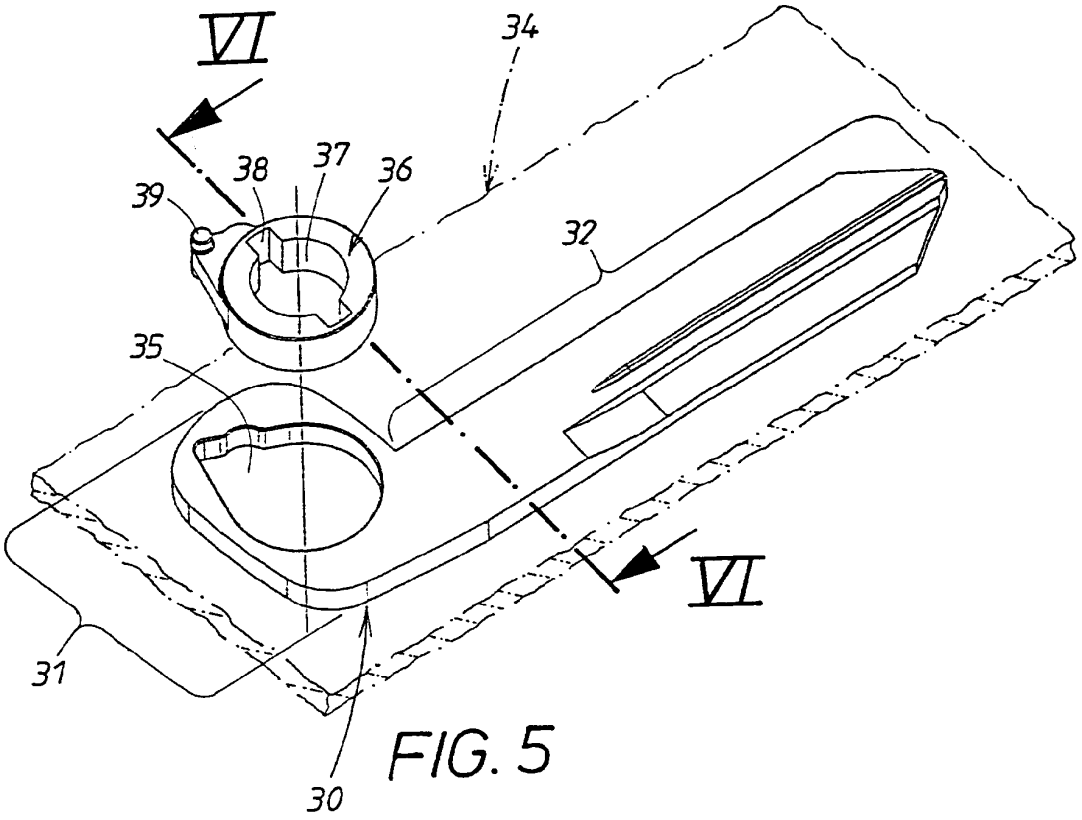


FIG. 5

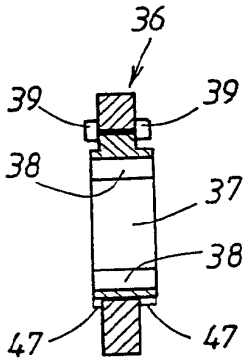


FIG. 6

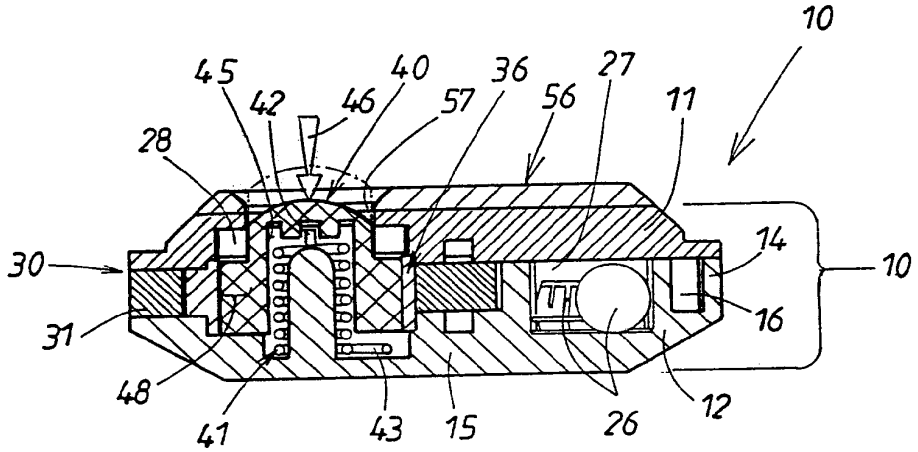

10
45
42
46
40
57
36
56
27
11
28
30
14
10
16
31
48
41
43
15
26
12

FIG. 7

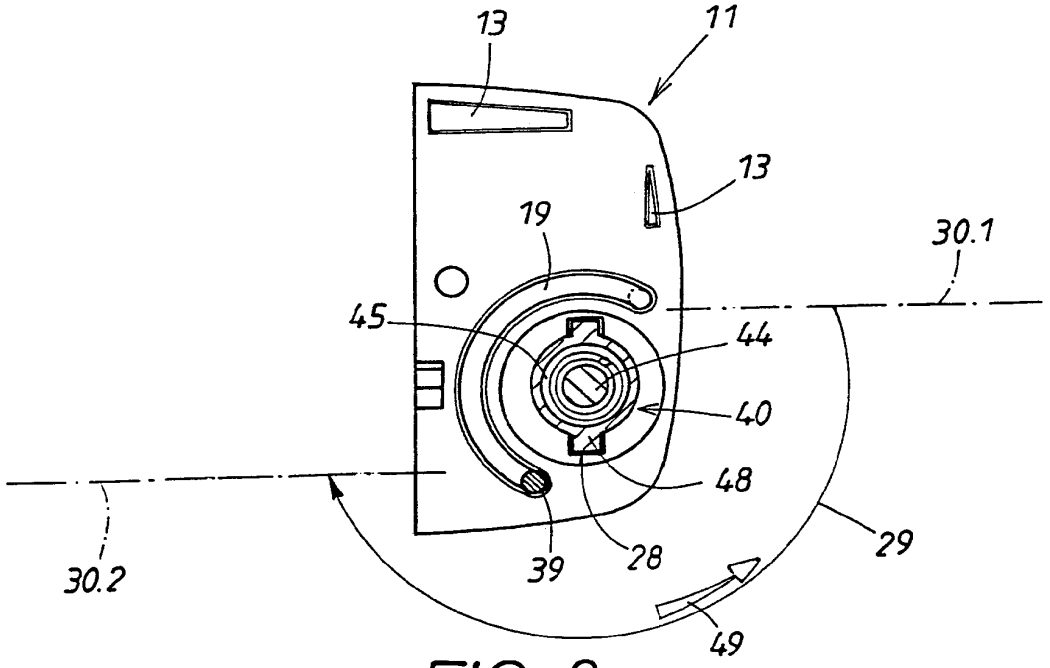

13
11
13
19
30.1
45
44
40
48
30.2
39
28
29
49

FIG. 8

INTERNATIONAL SEARCH REPORT

Internatic Application No
PCT/EP 00/11619

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 E05B19/04 E05B49/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 E05B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 42 26 579 A (MERCEDES-BENZ AG) 17 February 1994 (1994-02-17) column 4, line 38 -column 4, line 67; figures	1
A	WO 97 17863 A (POWELL) 22 May 1997 (1997-05-22) page 8, line 30 -page 11, line 14; figures	1
P,A	EP 0 985 788 A (VALEO ELECTRONIQUE) 15 March 2000 (2000-03-15) abstract; figures	1

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 May 2001	29/05/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Vacca, R

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internatic ' Application No
PCT/EP 00/11619

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 4226579 A	17-02-1994	NONE	
WO 9717863 A	22-05-1997	AU 7579796 A	05-06-1997
EP 985788 A	15-03-2000	FR 2783011 A	10-03-2000

IPR2022-00412
Apple EX1053 Page 628

INTERNATIONALER RECHERCHENBERICHT

Internatic ›s Aktenzeichen
PCT/EP 00/11619

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 E05B19/04 E05B49/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 E05B

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE 42 26 579 A (MERCEDES-BENZ AG) 17. Februar 1994 (1994-02-17) Spalte 4, Zeile 38 -Spalte 4, Zeile 67; Abbildungen	1
A	WO 97 17863 A (POWELL) 22. Mai 1997 (1997-05-22) Seite 8, Zeile 30 -Seite 11, Zeile 14; Abbildungen	1
P,A	EP 0 985 788 A (VALEO ELECTRONIQUE) 15. März 2000 (2000-03-15) Zusammenfassung; Abbildungen	1

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
17. Mai 2001	29/05/2001

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Vacca, R

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internatio s Aktenzeichen
PCT/EP 00/11619

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
DE 4226579	A	17-02-1994	KEINE		
WO 9717863	A	22-05-1997	AU	7579796 A	05-06-1997
EP 985788	A	15-03-2000	FR	2783011 A	10-03-2000

Formblatt PCT/ISA/210 (Anhang Patentfamilie)(Juli 1992)

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
5. Juli 2001 (05.07.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/48342 A1

(51) Internationale Patentklassifikation[7]: E05B 49/00, 19/00, 19/04

(21) Internationales Aktenzeichen: PCT/EP00/12431

(22) Internationales Anmeldedatum:
8. Dezember 2000 (08.12.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 62 976.5 24. Dezember 1999 (24.12.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **HUF HÜLSBECK & FÜRST GMBH & CO. KG** [DE/DE]; Steeger Strasse 17, 42551 Velbert (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **JACOB, Dirk** [DE/DE]; Breslauer Strasse 13, 42579 Heiligenhaus (DE). **MÜLLER, Ulrich** [DE/DE]; Schnegelskothen 7C, 42549 Velbert (DE).

(74) Anwalt: **MENTZEL, Norbert**; Kleiner Werth 34, 42275 Wuppertal (DE).

(81) Bestimmungsstaaten *(national)*: AU, BR, CN, IN, JP, KR, US.

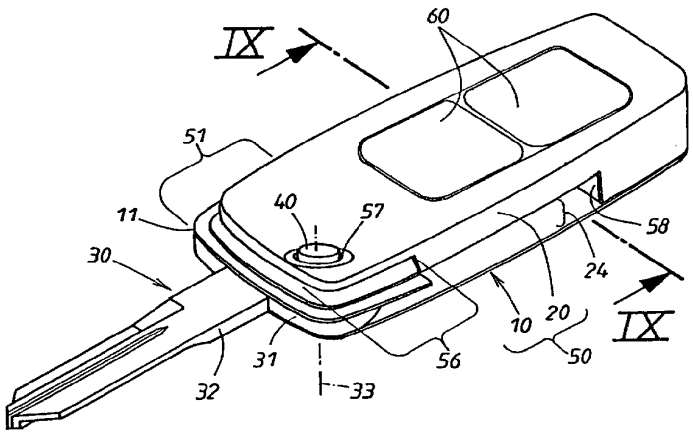
(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Veröffentlicht:
— *Mit internationalem Recherchenbericht.*

[Fortsetzung auf der nächsten Seite]

(54) Title: COMBINED MECHANICAL AND ELECTRONIC KEY, IN PARTICULAR FOR LOCKS IN A VEHICLE

(54) Bezeichnung: KOMBINIERTER MECHANISCHER UND ELEKTRONISCHER SCHLÜSSEL, INSBESONDERE FÜR AN FAHRZEUGEN BEFINDLICHE SCHLÖSSER



(57) Abstract: In a combined mechanical and electronic key, electronic components and mechanical flat keys (30) are normally housed in a common key holder (10). In order to place the flat key (30) between a lowered rest position in a holder (10) and a projecting in-use position, the flat key (30) is movably located in a container (10) and secured in at least one of said positions by a push button (40). The key container is assembled from an upper and a lower shell. In order to avoid sealing problems between both shells, according to the invention, the upper shell (11) is provided with an outbreak in a region pertaining thereto which lies outwith the push button.The outbreak creates a void chamber which can be accessed from the outside and is located on the inside of the shell interior. Said electronic components are enclosed by a housing-like capsule and form therewith a prefabricated electrocapsule (20). The electrocapsule (20) forms a socket unit, which can be inserted thereafter in the void chamber pertaining to the pre-assembled key container (10). The electrocapsules (10) are secured in the key container (10) when inserted in said socket. The push button (40) is used to advantage for securing.

[Fortsetzung auf der nächsten Seite]

WO 01/48342 A1

IPR2022-00412
Apple EX1053 Page 631

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Bei einem kombinierten mechanischen und elektronischen Schlüssel sind normalerweise die elektronischen Bauteile und der mechanische Flachschlüssel (30) in einem gemeinsamen Schlüsselbehälter (10) untergebracht. Um den Flachschlüssel (30) zwischen einen im Behälter (10) versenkten Ruhelage und einer herausragenden Gebrauchslage zu überführen, ist der Flachschlüssel (30) im Behälter (10) beweglich aufgenommen und in wenigstens einer dieser Lagen durch eine Druckknopf (40) arretiert. Der Schlüsselbehälter wird aus einer Ober- und Unterschale montiert. Um Dichtungsprobleme zwischen den beiden Schalen zu vermeiden, schlägt die Erfindung vor, die Oberschale (11) in ihrem ausserhalb des Druckknopfs (40) liegenden Bereich mit einem Ausbruch zu versehen. Der Ausbruch erzeugt einen von aussen zugänglichen Freiraum im Schaleninneren. Die elektronischen Bauteile sind von einer gehäuseartigen Kapsel umschlossen und bilden mit dieser eine vorgefertigte Elektrokapsel (20). Die Elektrokapsel (20) bildet eine Steckeinheit, welche nachträglich in den Freiraum des fertig montierten Schlüsselbehälters (10) einsteckbar ist. Im Einsteckfall ist die Elektrokapsel (10) im Schlüsselbehälter (10) gesichert. Vorteilhaft nutzt man den Druckknopf (40) für diese Sicherung aus.

IPR2022-00412
Apple EX1053 Page 632

Kombinierter mechanischer und elektronischer Schlüssel, insbesondere für an Fahrzeugen befindliche Schlösser

Die Erfindung richtet sich auf einen kombinierten Schlüssel der im Oberbegriff des Anspruches 1 angegebenen Art. Ein solcher Schlüssel erlaubt sowohl eine unmittelbare mechanische Betätigung der Schlösser als auch, alternativ oder ergänzend, eine elektronische Betätigung, z.B. eine Fernbedienung dieses Schlosses bzw. auch anderer Schlösser. Der Schlüsselbehälter ist das Handhabungsmittel sowohl zur mechanischen als auch elektrischen Schlüsselbetätigung. Für die elektronische Betätigung besitzt daher der Schlüsselbehälter an seiner Außenseite Betätigungsstellen, z.B. in Form von elektrischen Druckknöpfen oder nachgiebigen Membranen, die auf im Behälterinneren angeordnete elektrische Schalter od. dgl. einwirken. Der mechanische Flachschlüssel ist im Behälter beweglich aufgenommen und kann aus einer im Behälter versenkten Ruhelage in einer aus dem Behälter herausragenden Gebrauchslage überführt werden. Zur Lagesicherung empfiehlt es sich den Flachschlüssel in beiden Lagen durch einen im Behälter angeordneten axial gefederten Druckknopf zu arretieren.

IPR2022-00412
Apple EX1053 Page 633

Bei dem bekannten Schlüssel dieser Art (DE 39 02 537 C2) sind im Inneren des Schlüsselbehälters nicht nur der mechanische Flachschlüssel sondern auch die elektronischen Bauteile für die elektronische Betätigung unmittelbar angeordnet. Die elektronischen Bauteile umfassen auch die zur Energieversorgung dienenden Batterien, die nach längerem Gebrauch ausgewechselt werden müssen. Deswegen wird der Schlüsselbehälter aus einer Oberschale und aus einer Unterschale gebildet, die bedarfsweise voneinander gelöst werden müssen. Die Zerlegung und der Zusammenbau der Schalenteile sind schwierig und zeitaufwendig. Um den Flachschlüssel in der Ruhelage im Behälterinneren versteckt anzuordnen, ist eine seitliche Ausnehmung im Schlüsselbehälter vorgesehen, aus welcher der mechanische Flachschlüssel in seiner Gebrauchslage herausfährt. Durch die Fuge zwischen der Ober- und Unterschale können Schmutz und Feuchtigkeit ins Behälterinnere gelangen, weshalb es dort auf eine gute Dichtung ankommt. Diese Abdichtung ist aber nach längerer Gebrauchsdauer nicht immer gewährleistet, zumal wenn elektronische Bauteile oder Batterien ausgetauscht werden. Der Ausbau und das Einbringen der elektronischen Bauteile und der Batterien im Gehäuseinneren ist mühsam und zeitaufwendig. Bei der Zerlegung und dem Zusammenbau des Schlüsselbehälters mit seinen beiden Schalen besteht die Gefahr, dass die Dichtung nicht mehr ordnungsgemäß plaziert bzw. dabei beschädigt wird. Eine ähnliche Lösung mit den gleichen Nachteilen beschreibt die EP 0 267 429 A1.

Des Weiteren ist aus der GB 2 080 386 A bekannt, einen mechanischen Schlüssel mit einer aufsteckbaren Kassette zu versehen. Die aus zwei Schalen bestehende Kassette, die eine Lichtquelle enthält, bildet eine gehäuseartige Kapsel und kann als Steckeinheit nachträglich eingesteckt oder festgelegt werden. Der Schlüsselgriff besitzt dazu eine Ausnehmung, welche einen von außen zugänglichen Freiraum bildet. Nachteilig bei dieser Anordnung ist, dass die Steckeinheit in Einsteckposition nicht gesichert ist und sich einfach aus der Steckverbindung lösen kann.

IPR2022-00412
Apple EX1053 Page 634

Der Erfindung liegt die Aufgabe zugrunde, einen zuverlässigen, raumsparenden Schlüssel der im Oberbegriff des Anspruches 1 genannten Art zu entwickeln, bei dem es keine Dichtungsprobleme gibt und bei dem der Austausch von elektronischen Bauteilen und gegebenenfalls Batterien umproblematisch sind. Dies wird erfindungsgemäß durch die im Kennzeichen von Anspruch 1 erwähnten Maßnahmen erreicht, denen folgende besondere Bedeutung zukommt.

Die Erfindung braucht sich mit dem Dichtungsproblem zwischen der Ober- und Unterschale des Schlüsselbehälters nicht zu befassen, weil die auf Schmutz und Feuchtigkeit sehr empfindlichen elektronischen Bauteile, zu denen gegebenenfalls elektrische Batterien gehören, von einer gehäuseartigen Kapsel umschlossen sind, mit der sie eine vorgefertigte Baueinheit bildet, die nachfolgend kurz „Elektrokapsel" bezeichnet werden soll. Die in der Elektrokapsel befindlichen Elemente sind allseitig versiegelt. Bedarfsweise können die elektronischen Bauteile in der Elektrokapsel eingegossen sein. Diese Elektrokapsel ist dichtungsmäßig autark und bringt daher keine Dichtungsprobleme im Schlüsselbehälter. Die elektronischen Bauteile und ihre elektrischen Batterien sind im Inneren der Elektrokapsel nach außen geschützt untergebracht. Die Elektrokapsel wird ohne den zweischaligen Schlüsselbehälter zerlegen zu müssen, schnell und bequem in den Freiraum des Schlüsselbehälters eingesteckt und wieder entnommen werden. Die Elektrokapsel kann als eigenständiges Handelsprodukt in Verkehr gebracht werden, der vom Besitzer des Schlüssels erworben und mit dem stets geschlossen bleibenden Schlüsselbehälter zusammengesteckt werden kann.

Sowohl der Schlüsselbehälter mit seinem Ausbruch einerseits als auch die Elektrokapsel andererseits werden für sich vorgefertigt und sind jederzeit miteinander montierbar bzw. voneinander demontierbar. Weil der Schlüsselbehälter nicht in seine beiden Schalen zerlegt zu werden braucht, treten dort keine Dichtungsprobleme auf. Im übrigen ist es unmaßgeblich, ob bei eingesteckter Elektrokapsel der Schlüsselbehälter abgedichtet ist, denn dort

befinden sich nur die hinsichtlich Schmutz und Feuchtigkeit unempfindlichen Bauteile, wie der mechanische Flachschlüssel. Der Ausbruch im Schlüsselbehälter wird von der eingesteckten Elektrokapsel verschlossen. Die Elektrokapsel vervollständigt den Schlüsselbehälter zu einem bei der Schlüsselbetätigung gemeinsam zu handhabenden Kombinationsgehäuse. Die zur Handhabung dienende Fläche des Kombinationsgehäuses wird also teils vom Schlüsselbehälter des mechanischen Flachschlüssels und teils von der freibleibenden Umfangsfläche der Elektrokapsel gebildet. An den Übergangsstellen wird man für einen bündigen Übergang sorgen.

Weitere Maßnahmen und Vorteile der Erfindung ergeben sich aus den Unteransprüchen, der nachfolgenden Beschreibung und den Zeichnungen. In den Zeichnungen ist die Erfindung in einem Ausführungsbeispiel schematisch dargestellt. Es zeigen:

Fig. 1, in perspektivischer Darstellung, den Schlüsselbehälter mit herausragendem mechanischen Flachschlüssel,

Fig. 2, ebenfalls in perspektivischer Darstellung, eine zum Flachschlüssel von Fig. 1 gehörende Steckeinheit, bestehend aus einer die elektronischen Bauteile umschließenden Elektrokapsel,

Fig. 3 ein aus dem Schlüsselbehälter von Fig. 1 und der Steckeinheit von Fig. 2 zusammengestecktes Kombinationsgehäuse, das zur Handhabung bei mechanischer und elektronischer Betätigung des Schlüssels dient,

Fig. 4, in Explosionsdarstellung, einige wesentliche Bestandteile des in Fig. 1 gezeigten Schlüsselbehälters mit dem mechanischen Flachschlüssel, vor deren Zusammenbau,

IPR2022-00412
Apple EX1053 Page 636

Fig. 5, in Explosionsdarstellung, die beiden Bestandteile des mechanischen Flachschlüssels vor ihrer Vereinigung,

Fig. 6 einen Querschnitt durch den einen Bestandteil von Fig. 5, längs der dortigen Schnittlinie VI - VI,

Fig. 7 einen Querschnitt durch das zusammengebaute Schlüsselbehälter von Fig. 1 längs der dortigen Schnittlinie VII - VII, wobei ein Druckknopf in seiner eingedrückten Position gezeigt ist,

Fig. 8 einen Axialschnitt durch den in Fig. 1 gezeigten Schlüsselbehälter längs der dortigen Schnittlinie VIII - VIII und

Fig. 9 einen Querschnitt durch das in Fig. 3 gezeigte Kombinationsgehäuse längs der dortigen Schnittlinie IX - IX.

Der kombinierte Schlüssel nach der Erfindung erlaubt sowohl eine mechanische als auch eine elektronische Betätigung eines nicht näher gezeigten Schlosses. Er besteht aus zwei jeweils für sich vorgefertigten Teilen 10, 20, die nachträglich ineinandergefügt werden. Der eine Teil 10 umfasst die mechanischen Schließmittel und besteht aus einem Schlüsselbehälter 10, dessen Bestandteile aus der Explosionsdarstellung von Fig. 4 am besten zu erkennen sind. Der andere Teil 20 ist eine noch näher zu beschreibende Steckeinheit, welche die in ihrem Inneren die im Querschnitt von Fig. 9 angedeuteten elektronischen Bauteile 40 umfasst.

Ausweislich der Fig. 1 und 4 umfasst der mechanische Teil zunächst einen zweischaligen Schlüsselbehälter 10. Während die Oberschale 11, wie Fig. 7 und 8 erkennen lässt, als ebene Platte mit stellenweisen Kupplungsvorsprüngen 13 an

IPR2022-00412
Apple EX1053 Page 637

ihrer Innenfläche ausgebildet ist, umfasst die Unterschale 12 außer ihrem Schalenboden 15 auch noch Schalenseitenwände 14. In den Schalenseitenwänden 14 befinden sich stellenweise Kupplungsaufnahmen 16 für die vorerwähnten Kupplungsvorsprünge 13 der Oberschale 11. Die Oberschale 11 erstreckt sich nur über einen vorderen Bereich des Schlüsselbehälters 10 und weist im hinteren Bereich einen Ausbruch 17 auf, der zum Schaleninneren 18 hin einen von außen zugänglichen Freiraum erzeugt. Das ist für das noch näher zu beschreibende Einstecken bzw. Herausziehen der Steckeinheit 20 bedeutungsvoll.

Zum Schlüsselbehälter 10 gehört, wie Fig. 4 zeigt, ein mechanischer Flachschlüssel 30 der beweglich angeordnet ist, um aus einer nicht näher gezeigten versenkten Ruhelage im Behälter 10 in eine aus dem Behälter herausragenden, in Fig. 1 bis 4 ersichtliche Gebrauchslage überführt zu werden. Der Flachschlüssel 30 besteht aus metallischem Werkstoff. Obwohl auch andere Bewegungen denkbar wären, ist dieser Flachschlüssel 30 um die strichpunktiert in den Fig. 1, 3 und 4 angedeuteten Schwenkachsen 33 schwenkbeweglich. Dabei ist der Flachschlüssel 30 als ein Stanzling aus einer in Fig. 4 strichpunktiert verdeutlichten ebenen Platte 34 ausgebildet, wobei der Stanzling ein L-förmiges Umrissprofil aus zwei Schenkeln 31, 32 besitzt. Der eine L-Schenkel ist kurz ausgebildet und dient zur Schwenklagerung des Flachschlüssels 30 am Vorderende des Schlüsselbehälters 10 und wird daher nachfolgend kurz „Lagerschenkel" genannt. Der andere L-Schenkel 32 umfasst das eigentliche Flachprofil des Schlüsselschafts, weshalb er nachfolgend als „Schaftschenkel" bezeichnet werden soll. Beide Schenkel 31, 32 liegen also in einer gemeinsamen, durch den erwähnten Plattenverlauf 34 bestimmten Ebene, die im fertig montierten Zustand des Schlüsselbehälters 10 senkrecht zur Schwenkachse 33 verläuft. Ausweislich der Fig. 5 ist der Lagerschenkel 31 mit einem unrunden Plattendurchbruch 35 versehen, der zur Aufnahme eines besonderen Einsatzes 36 dient.

Der Druckknopf 40 ist sowohl axial als auch radial federbelastet und besitzt mit dem Behälter 10 übereinstimmend ausgebildete Profile 19, 48, 28. Der Einsatz 36

besteht aus relativ nachgiebigem Material, vorzugsweise Kunststoff und besitzt ein besonderes Gegenprofil 37, 38, 39 für einen die Lage der Schwenkachse 33 bestimmenden Druckknopf 40. Die Federwirkung übernimmt eine kombinierte Druck-Dreh-Feder 41, die, ausweislich der Fig. 7, in einer Axialbohrung 45 des Druckknopfs 40 aufgenommen ist. Die Feder 41 ist mit ihrem einen Federende 42 drehfest mit dem Druckknopf 40 verbunden, während ihr anderes Federende 43 in der Unterschale 12 des Behälters 10 festgehalten wird. Die Feder 41 ist wendelförmig ausgebildet. Im Montagefall greift ein an der bodenseitigen Innenfläche der Unterschale 12 sitzender Dorn 44 sowohl ins Wendelinnere hinein, als auch in den Einsatz 36 ein.

Gemäß Fig. 5 wird zunächst der Flachschlüssel 30 mit seinem Plattendurchbruch 35 durch Stanzen erzeugt und dann, nachträglich, der Einsatz 36 in den Plattendurchbruch 35 vertikal eingesteckt. Nach diesem Einstecken ragt, wie Fig. 4 und 7 zeigen, über die beiden Plattenflächen des Flachschlüssels heraus. Dazu gehören zylindrische Ansätze 47, gemäß Fig. 6, aber auch ein Anschlagzapfen 39 an beiden Flächenseiten, der in ein Ringnutsegment 19 der beiden Schalen 11 und 12 hineinragt, wie aus Fig. 8 zu entnehmen ist. In der in Fig. 8 ausgezogen gezeichneten Position des Anschlagnockens 39 liegt die bereits eingangs erwähnte, aus dem Behälter 10 herausgeschwenkte Gebrauchslage vor. Dann erstreckt sich der vorbeschriebene Schaftschenkel 32 des Flachschlüssels 30 in Richtung der in Fig. 8 strichpunktiert angedeuteten Hilfslinie 30.1, welche die in den übrigen Fig. dargestellte Gebrauchslage des Flachschlüssels 30 kennzeichnet. In dieser Gebrauchslage 30.1 ist der Flachschlüssel durch den Druckknopf 40 arretiert. Dann greifen am Druckknopf 40 vorgesehene, hier diametral angeordnete Mitnahmeflügel 48 in zugehörige Radialnuten 28 an der Innenfläche der Oberschale 11 hinein und sichern so die Ausschwenklage des Flachschlüssels 30.

Die Mitnahmeflügel 48 besitzen, als Gegenprofil, im Einsatz 36 Axialnuten 48, die eine Eindruckbewegung im Sinne des aus Fig. 7 erkennbaren Kraftpfeils 46 zulassen. Diese Eindruckbewegung 46, die in Fig. 7 vollzogen ist, führt zu einer

IPR2022-00412
Apple EX1053 Page 639

axialen Absenkung des Druckknopfs 40, wodurch die Mitnahmeflügel 48 die Radialnuten 28 freigeben. Die Eindruckbewegung 46 erfolgt gegen die axiale Kraftwirkung der Feder 41. Die Arretierung der Gebrauchslage 30.1 ist dann aufgehoben. Der Flachschlüssel kann dann im Sinne des Bewegungspfeils 29 von Fig. 8 gegen die durch den Kraftpfeil 49 in Fig. 8 verdeutlichte Drehkraft der Feder 41 in seine Ruhelage im Gehäuse zurückgeschwenkt werden. Dann liegt der Schaftschenkel 32 des Flachschlüssels 30, in Fig. 8 gesehen, an der dort mit 30.2 gekennzeichneten Strichpunktlinie. In dieser Ruhelage 30.2 verschwindet der Schaftschenkel 32 in einem aus Fig. 3 erkennbaren seitlichen Spalt 24 eines noch näher zu beschreibenden Gesamtgehäuses 50, welches aus dem Schlüsselbehälter 10 und der darin eingeschobenen Steckeinheit 20 entsteht. Dann sind die Mitnahmeflügel 48 wieder in axialer Ausrichtung mit den gehäuseseitigen Radialnuten 28, wo sie durch die Rückstellkraft der Feder 41 einschnappen und so auch diese Ruhelage 30.2 des Flachschlüssels 30 im Schlüsselbehälter 10 arretieren.

Bei der Schwenkbewegung 29 dient der Druckknopf 40 auch als Schwenklager. Dazu ist in der Oberschale 11 des Behälters 10 eine aus Fig. 4 erkennbare Lagerbohrung 25 vorgesehen. Diese ist in axialer Ausrichtung mit einer in Fig. 5 und 6 gezeigten Axialbohrung 37 des Einsatzes 36 und mit dem bereits mehrfach erwähnten Dorn 44 der Unterschale 12. Der Druckknopf 40 bestimmt die Schwenkachse 33 des Flachschlüssels 30. Der Anschlagzapfen 39 vom Einsatz 36 einerseits und das ihm gehäuseseitig zugeordnete Ringnutsegment 19 andererseits können auch Drehführungsfunktionen bei der Schwenkbewegung 29 übernehmen. Außerdem können Drehanschläge durch das Umrissprofil des Schlüssels 30 einerseits und Innenflächen an den beiden Schalen 11, 12 andererseits verwirklicht sein.

Statt einer Vorfertigung des Einsatzes 36 könnte man den Einsatz 36 durch eine Spritzgusstechnik nachfertigen. Dazu wird der beschriebene Flachschlüssel 30 in eine Spritzgussform eingebracht, in welcher dann der Einsatz 36 im

Plattendurchbruch 35 durch Gießen gebildet wird. Die erwähnte Gegenprofilierung 37, 38, 39, 47 liegt dann in ähnlicher Form vor.

In manchen Anwendungsfällen ist bei dem eingangs erwähnten kombinierten Schlüssel für die elektronische Betätigung auch ein sogenannter Transponder 26 erwünscht. Dieser Transponder 26 soll bereits zur elektronischen Individualisierung dieses kombinierten Schlüssels sorgen. Wird dieser Schlüssel in das zugehörige Schloss eingesteckt, so findet zwischen dem Transponder 26 und dem Schloss eine Kommunikation statt, die bei Übereinstimmung von Schloss und Schlüssel bereits Schlossfunktionen auslöst. Deswegen werden bei der Erfindung derartige Transponder 26 im vorderen Bereich des Schlüsselbehälters 10 untergebracht. Dazu besitzt die Unterschale 12 eine Kammer 27, in welche der bzw. die Transponder 26 eingeklebt werden können. Weil eine elektronische Energieversorgung der Transponder 26 nicht erforderlich ist, braucht der fertig montierte Schlüsselbehälter 10 von Fig. 1 nicht mehr in seine Schalen 11, 12 zerlegt zu werden, um dort einen Batteriewechsel od. dgl. vorzunehmen. Die Transponder 26 sind also in der Kammer 27 permanent geschützt. Das gilt auch für die bereits eingangs erwähnten weiteren elektronischen Bauteile 21, welche innerer Bestandteil der bereits erwähnten lösbaren Steckeinheit 20 des Gesamtgehäuses 50 sind.

Wie am besten aus Fig. 9 zu ersehen ist, gehören zur Steckeinheit 20 eine gehäuseartige Kapsel 22, in deren Innenraum 23 die Bauteile 21 angeordnet und so nach außen allseitig abgeschlossen sind. Im Kapselinneren 23 können auch die Schaltungen der Bauelemente und gegebenenfalls die elektrische Störung angeordnet sein. Diese Baueinheit 21, 22, die als Steckeinheit mit dem Schlüsselbehälter 10 fungiert, wird komplett vorgefertigt und soll nachfolgend „Elektrokapsel" genannt werden. Dazu ist der Schlüsselbehälter 10 profilmäßig in folgender Weise angepasst.

IPR2022-00412
Apple EX1053 Page 641

Der eingangs erwähnte Ausbruch 17 im Schlüsselbehälter 10 erfolgt einfach dadurch, dass die Oberschale 11, gemäß Fig. 1, nur den Vorderabschnitt 51 des Schlüsselbehälters 10 überdeckt. Dadurch ist ein von außen zugänglicher Freiraum ins Schaleninnere 18 erzeugt. Dieser Freiraum 17 besitzt nicht nur eine nach oben weisende Oberöffnung 52, sondern erstreckt sich auch in eine vom Hinterende 54 zugängliche Seitenöffnung 53. Diese entsteht, weil nicht nur der hintere Abschnitt der Oberschale 11 fehlt, sondern auch, wie Fig. 1 zeigt, die Seitenwand 14 der Unterschale 12 am Hinterende 54 des Behälters 10 weggefallen ist. Die Elektrokapsel 20 wird durch diese Seitenöffnung 53 in den Freiraum 17 des Schlüsselbehälters 10 gemäß dem Bewegungspfeil 55 von Fig. 1 eingeschoben. In ihrer Einschublage, gemäß Fig. 3, verschließt die Elektrokapsel 20 die Oberöffnung 52. Die Einschubbewegung 55 ist in einer Parallelebene zu der oben erwähnten Schwenkbewegung 29 angeordnet. Dabei sind folgende Führungsmittel 61, 62 zum gezielten Einstecken und Verschieben 55 der Elektrokapsel 20 vorgesehen.

An der Innenfläche des Schalenbodens 15 der Unterschale 12 befinden sich zwei parallele Führungsleisten 61, die zur Seitenöffnung 53 hin gerichtet sind. Sie sind hinterschnitten und besitzen vorzugsweise ein schwalbenschwanzförmiges Profil. Ihnen sind angepasste Führungsnuten 62 an der Unterseite des Gehäuses der Elektrokapsel 20 zugeordnet. Die Eingriffslage dieser Führungsmittel 61, 62 ist im Schnitt von Fig. 9 zu erkennen. Dabei ist die eine Längsseite vom Kapselgehäuse 22 gemäß Fig. 9 bei 58 gestuft, so dass mit einer entsprechenden Stufung 59 in der Unterschale 12, gemäß Fig. 4, in der Einschublage der seitliche Spalt 24 für den Schaftschenkel 32 des Flachschlüssels 30 entsteht. In der Einschublage gemäß Fig. 3 und 9 gehen die sichtbar bleibenden Außenflächen der Elektrokapsel 20 einerseits und des Schlüsselbehälters 10 andererseits ineinander bündig über. Beide Teile 10, 20 bilden dann das bereits erwähnte Kombinationsgehäuse 50, welches beim Handhaben des Schlüssels mit der Hand gemeinsam umgriffen wird und daher „Kombinationsgehäuse“ genannt werden soll. Dies gilt sowohl bei einer mechanischen Betätigung des zugehörigen Schlosses, wo der herausgeschwenkte

IPR2022-00412
Apple EX1053 Page 642

Schaftschenkel 32 mittels des Kombigehäuses 50 gedreht wird, als auch bei der elektronischen Betätigung. Dafür sind Betätigungsstellen 60 an die sichtbar bleibende Außenfläche der Elektrokapsel 20 im gemeinsamen Kombinationsgehäuse 50 vorgesehen. Diese können aus Druckschaltern oder membranartigen Betätigungsstellen entstehen. Diese Betätigungsstellen können mit weiteren membranartigen Überdeckungen im Bereich des vorerwähnten Druckknopfs 40 vorgesehen sein, dem noch folgende besondere Bedeutung zukommt.

Die in Fig. 3 und 9 gezeigte Einstecklage der Elektrokapsel 20 im Schlüsselbehälter 10 ist nicht nur durch Anschlagmittel begrenzt, sondern auch durch Rastmittel gesichert. Diese Funktion kann in vorteilhafterweise auch vom Druckknopf 40 übernommen werden. Dazu ist die Elektrokapsel 20, gemäß Fig. 2, vorderendig mit einem Lappen 56 verlängert, der in der Einschublage von Fig. 3 den verbliebenen Vorderabschnitt 51 der Oberschale 11 vom Schlüsselbehälter 10 überdeckt. Der Lappen 56 besitzt eine Ausnehmung 57, in welche der axial federnde Druckknopf 40 in der Einschublage der Elektrokapsel 20 gemäß Fig. 3 einschnappt. Dadurch ist der Zusammenhalt des Schlüsselbehälters mit der Elektrokapsel 20 sichergestellt. Die Ausnehmung 57 durchsetzt den Lappen 56, weshalb im Eingriffsfall gemäß Fig. 3 der Druckknopf 40 mit einem zu seiner Betätigung ausreichenden Längenstück aus dem Lappen 56 herausragt. Zur Demontage des Kombinationsgehäuses 50 in seine Bestandteile 10, 20 wird der Druckknopf 40, wie Fig. 7 zeigt, soweit im Sinne des Pfeils 46 eingedrückt, dass er die Ausnehmung 57 im Lappen 56 freigibt.

Der Druckknopf 40 kann durch eine Membran im Bereich des Lappens 56 überdeckt sein, welche in ähnlicher Weise wie die Betätigungsstellen 61 fungiert. Diese Membrane dieser Betätigungsstellen 61 können mit der vorgenannten Membran im Bereich des Druckknopfs 40 kombiniert sein.

IPR2022-00412
Apple EX1053 Page 643

Bezugszeichenliste :

10	erster Schlüsselteil, Schlüsselbehälter
11	Oberschale von 10
12	Unterschale von 10
13	Kupplungsvorsprung an 11
14	Schalenseitenwand von 12
15	Schalenboden von 12
16	Kupplungsaufnahme von 12
17	Ausbruch von 11, Freiraum in 18
18	Schaleninneres
19	Profil in 11, 12 für 39, Ringnutsegment
20	zweiter Schlüsselteil, Steckeinheit, Elektrokapsel
21	elektronischer Bauteil
22	gehäuseartige Kapsel für 21
23	Kapselinneres für 22 in 21
24	seitlicher Spalt in 50 für 32 (Fig. 3, 9)
25	Lagerbohrung in 11 für 40 (Fig. 4)
26	Transponder
27	Kammer in 11 für 26 (Fig. 4)
28	Profil in 11 für 48 von 40, Radialnut (Fig. 7)
29	Schwenkbewegungspfeil für 30 (Fig. 8)
30	mechanischer Flachschlüssel für 10, Stanzling
30.1	Gebrauchslage von 32 (Fig. 8)
30.2	Ruhelage von 32 (Fig. 8)
31	erster L-Schenkel von 30, Lagerschenkel
32	zweiter L-Schenkel von 30, Schaftschenkel
33	Schwenkachse für 30
34	ebene Platte für 30
35	Plattendurchbruch

IPR2022-00412
Apple EX1053 Page 644

36	Einsatz in 35
37	Gegenprofil in 36, Axialbohrung (Fig. 5, 6)
38	Gegenprofil von 36, Axialnut in 36 für 48 (Fig. 5, 8)
39	Gegenprofil von 36, Führungs- bzw. Anschlagzapfen (Fig. 5, 6)
40	Druckknopf
41	Druck-Dreh-Feder von 40
42	erstes Federende von 41 (Fig. 7)
43	zweites Federende von 41 (Fig. 7)
44	Dorn an 12 für 41 (Fig. 4)
45	Axialbohrung in 40 für 41
46	Pfeil der Eindruckbewegung von 40 (Fig. 7)
47	Gegenprofil an 36, zylindrischer Ansatz an 36 (Fig. 5)
48	Profil, Mitnahmeflügel an 40
49	Pfeil der Ausschwenkkraft von 41 für 30 (Fig. 8)
50	Gesamtgehäuse aus 10, 20, Kombinationsgehäuse
51	Vorderabschnitt von 10
52	Oberöffnung von 10 bei 17 (Fig. 1)
53	Seitenöffnung von 11 (Fig. 1)
54	Hinterende von 10
55	Pfeil der Einschubbewegung von 20 in 10 (Fig. 1)
56	Lappen an 20 (Fig. 2)
57	Ausnehmung in 56 für 40 (Fig. 2)
58	Innenstufung von 22 für 24 (Fig. 2, 9)
59	Stufe von 12 für 24 (Fig. 4)
60	Betätigungsstelle an 20 (Fig. 1)
61	Führungsmittel an 12, Führungsleiste
62	Führungsmittel an 20, Führungsnut

Patentansprüche:

1.) Kombinierter mechnischer und elektronischer Schlüssel, insbesondere für in Fahrzeugen befindliche Schlösser,

mit einem gemeinsamen, bei der Schlüsselbetätigung zu handhabenden Schlüsselbehälter (10) sowohl für elektronische Bauteile (21) zur elektronischen Betätigung als auch für einen Flachschlüssel (30) zur mechanischen Betätigung des Schlosses,

wobei der Flachschlüssel (30) im Behälter beweglich (29) aufgenommen ist und aus einer im Behälter (10) versenkten Ruhelage (30.2) in eine aus dem Behälter (10) herausragende Gebrauchslage (30.1) überführbar ist,

und mit einem im Behälter (10) angeordneten axial gefederten (41) Druckknopf (40), der den Schlüssel (30) in wenigstens einer dieser Lagen (30.1; 30.2) arretiert,

wobei der Schlüsselbehälter (10) aus einer Ober- und Unterschale (11, 12) besteht, die wenigstens bereichsweise aneinander befestigt sind,

dadurch gekennzeichnet,

daß die Oberschale (11) in ihrem außerhalb des Druckknopfs (40) liegenden Bereich einen Ausbruch (17) aufweist,

IPR2022-00412
Apple EX1053 Page 646

daß der Ausbruch einen von außen zugänglichen Freiraum (17) im Schaleninneren (18) erzeugt,

daß die elektronischen Bauteile (21), deren Schaltung und gegebenenfalls elektrische Steuerung von einer gehäuseartigen Kapsel (22) umschlossen sind und mit dieser eine vorgefertigte

daß die Elektrokapsel (20) eine Steckeinheit bildet, welche nachträglich in den Freiraum (17) des fertig montierten Schlüsselbehälters (10) einsteckbar (55) und dort festlegbar ist,

daß die Elektrokapsel (20) einen sie vorderendig verlängerten Lappen (56) besitzt,

daß in der Einschublage der Kapsel (20) der Lappen (56) das vor der Oberöffnung (52) des Schlüsselbehälters befindliche Raststück (51) der Oberschale (11) wenigstens bereichsweise überdeckt,

und daß der Lappen (56) eine Ausnehmung (57) aufweist, in welcher der federnde (41) Druckknopf (40) axial einfährt und die Einschublage der Elektrokapsel (20) im Schlüsselbehälter (10) sichert.

2.) Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass die eingesteckte Elektrokapsel (20) auf ihrer im Ausbruch (17) freiliegenden Flächenbereichen Betätigungsstellen (60) zum Wirksamsetzen der in ihrem Inneren befindlichen elektronischen Bauteile (21) besitzt.

3.) Schlüssel nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die eingesteckte Elektrokapsel (20) den Ausbruch (17) im Schlüsselbehälter (10) verschließt

und dass die Steckkombination aus der Elektrokapsel (20) einerseits und dem Schlüsselbehälter (20) andererseits ein Kombinationsgehäuse (50) mit bündig übergehender Umfangsfläche erzeugt.

4.) Schlüssel nach einem oder mehreren der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass der Ausbruch (17) nicht nur eine nach oben weisende Oberöffnung (52) erzeugt, die durch Wegfall des hinteren Oberschalen-Abschnitts entsteht, sondern sich auch über eine Seitenöffnung (53) erstreckt, die durch einen wenigstens bereichsweisen Wegfall der Seitenwand (14) in der Unterschale (12) und gegebenenfalls in der Oberschale (11) entsteht,

dass die Elektrokapsel (20) durch die Seitenöffnung (53) in den Freiraum (17) des Schlüsselbehälters (10) einschiebbar (55) ist und in ihrer Einschublage auch die Oberöffnung (52) wenigstens bereichsweise verschließt.

5.) Schlüssel nach einem oder mehreren der Ansprüche 1 bis 4, wobei der Flachschlüssel (30) zwischen seiner Ruhe- und Gebrauchslage (30.2; 30.1) im Behälter (10) verschwenkbar (29) ist,

wobei der Druckknopf (40) als Schwenklager (33) für den Flachschlüssel (30) dient und seine Federung (41) bestrebt (49) ist, den Flachschlüssel (30) in dessen Gebrauchslage (30.1) herauszuschwenken,

dadurch gekennzeichnet,

dass die Einschubrichtung (55) der Elektrokapsel (50) in den Schlüsselbehälter (10) in einer Parallelebene zur Schwenkbewegung (29) des Flachschlüssels (30) angeordnet ist.

6.) Schlüssel nach Anspruch 4 oder 5, dadurch gekennzeichnet, dass die zum Einschub (55) der Elektrokapsel (20) dienende Seitenöffnung (53) sich an dem bezüglich des Druckknopfs (40) gegenüberliegenden Hinterende (54) des Schlüsselbehälters (10) befindet.

7.) Schlüssel nach einem oder mehreren der Ansprüche 4 bis 6, dadurch gekennzeichnet, dass die Unterschale (12) und die Elektrokapsel (20) Führungsmittel (61, 62) zum gezielten Einstecken und Verschieben (55) der Elektrokapsel (20) besitzen

und dass die Führungsmittel (61, 62) zur Seitenöffnung (53) der Unterschale (12) hin weisen.

8.) Schlüssel nach Anspruch 7, dadurch gekennzeichnet, dass die Führungsmittel (61, 62) in der Unterschale (12) zur Oberöffnung (52) des Schlüsselbehälters (10) hin hinterschnitten sind.

9.) Schlüssel nach Anspruch 7 oder 8, dadurch gekennzeichnet, dass die Führungsmittel aus mindestens einer, vorzugsweise aber zwei Führungsleisten (61) bestehen, die ein schwalbenschwanzförmiges Profil besitzen,

IPR2022-00412
Apple EX1053 Page 649

und dass die Elektrokapsel (20) dazu angepasste Führungsnuten (62) besitzt.

10.) Schlüssel nach einem oder mehreren der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass die Einstecklage der Elektrokapsel (20) im Schlüsselbehälter (10) durch Anschlagmittel begrenzt und durch Rastmittel gesichert ist.

11.) Schlüssel nach Anspruch 11, dadurch gekennzeichnet, dass die Ausnehmung (57) den Lappen (56) durchsetzt

und dass der Druckknopf (40) in der Einschublage der Elektrokapsel (20) mit seinem Betätigungsende zu Betätigungszwecken aus der Lappenoberseite herausragt.

12.) Schlüssel nach Anspruch 11 oder 12, dadurch gekennzeichnet, dass am Druckknopf (40) und an seiner Aufnahme (44) im Schlüsselbehälter (10) Steuermittel (41, 48, 38, 37) angeordnet sind, die den Druckknopf (40) während der Schwenkbewegung (29) des Flachschlüssels (30) zwischen der Gebrauchs- und Ruhelage (30.1; 30.2) in einer axial eingedrückten Position halten,

und dass der Druckknopf (40) in dieser Eindrückposition aus der Ausnehmung (57) im Lappen (56) ausgefahren ist und die Elektrokapsel (20) freigibt.

IPR2022-00412
Apple EX1053 Page 650

13.) Schlüssel nach einem oder mehreren der Ansprüche 11 bis 13, dadurch gekennzeichnet, dass der Lappen (56) im Bereich seiner Ausnehmung (57) eine Membran aufweist, welche in Einschublage der Elektrokapsel (20) den Druckknopf (40) nach oben überdeckt,

und dass diese Membran die manuelle Betätigungsstelle für den Druckknopf (40) bildet.

14.) Schlüssel nach Anspruch 13 oder 14, dadurch gekennzeichnet, dass die Membran mit dem Lappen (56) der Elektrokapsel (20) einstückig ausgebildet ist.

15.) Schlüssel nach Anspruch 14 oder 15, dadurch gekennzeichnet, dass die zur Betätigung des Druckknopfs (40) dienende Membran mit weiteren membranartigen Betätigungsstellen (60) im Schlüsselgehäuse (10) bzw. an der im Einsteckfall sichtbar bleibenden Außenfläche der Elektrokapsel (20) kombiniert ist, die zum Wirksamsetzen der elektronischen Bauteile (21) in der Elektrokapsel (20) dienen.

IPR2022-00412
Apple EX1053 Page 651

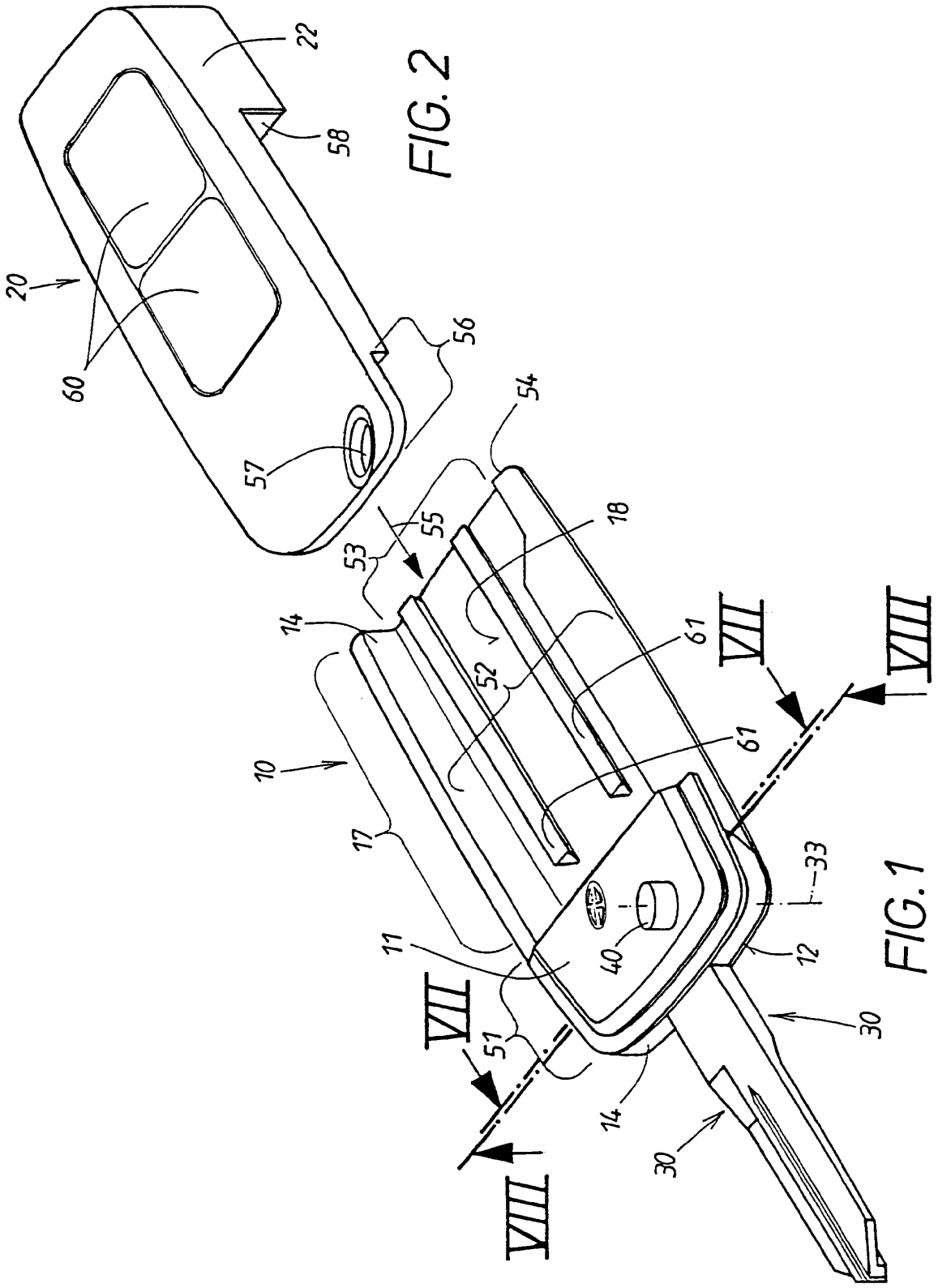

22
58
20
60
56
57
54
55
53
18
14
52
61
VII
VIII
10
17
11
40
33
12
30
51
VII
VIII
14
30

FIG. 2

FIG. 1

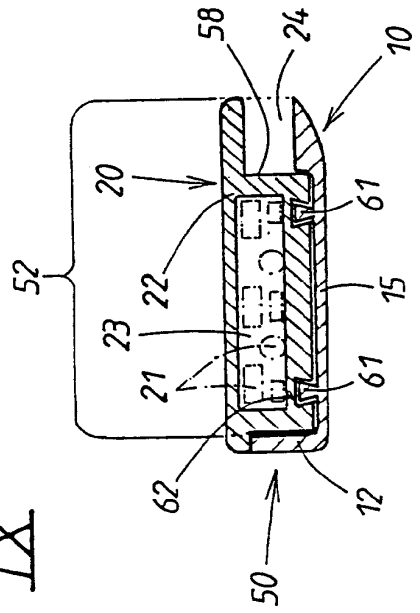

58
24
10
20
61
52
22
15
23
21
61
62
12
50

FIG. 9

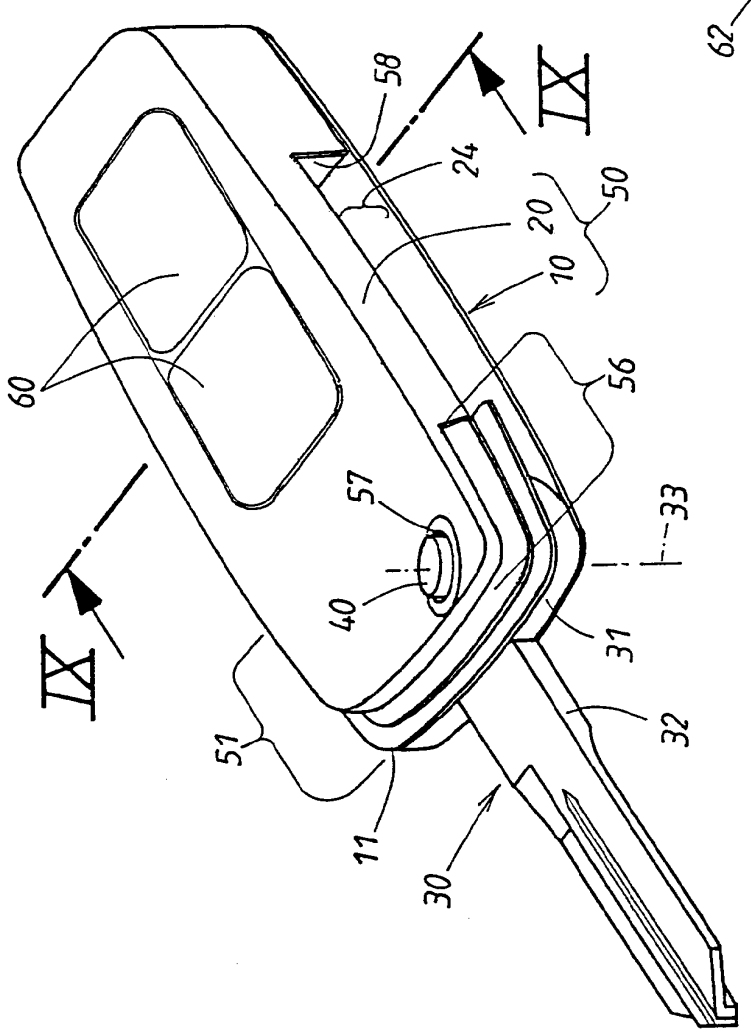

IX
58
24
20
50
10
60
56
57
33
40
31
IX
51
32
11
30

FIG. 3

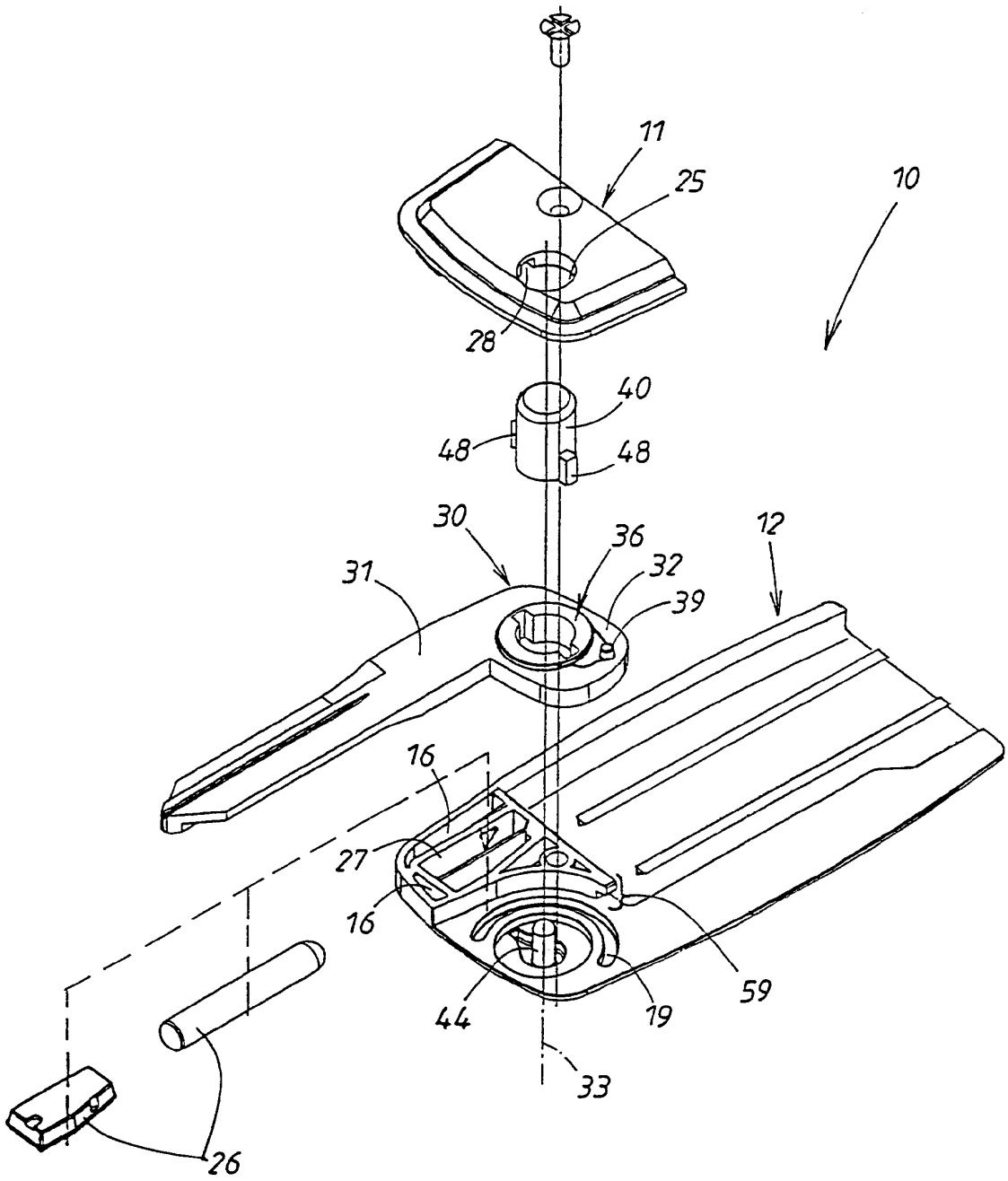


FIG. 4

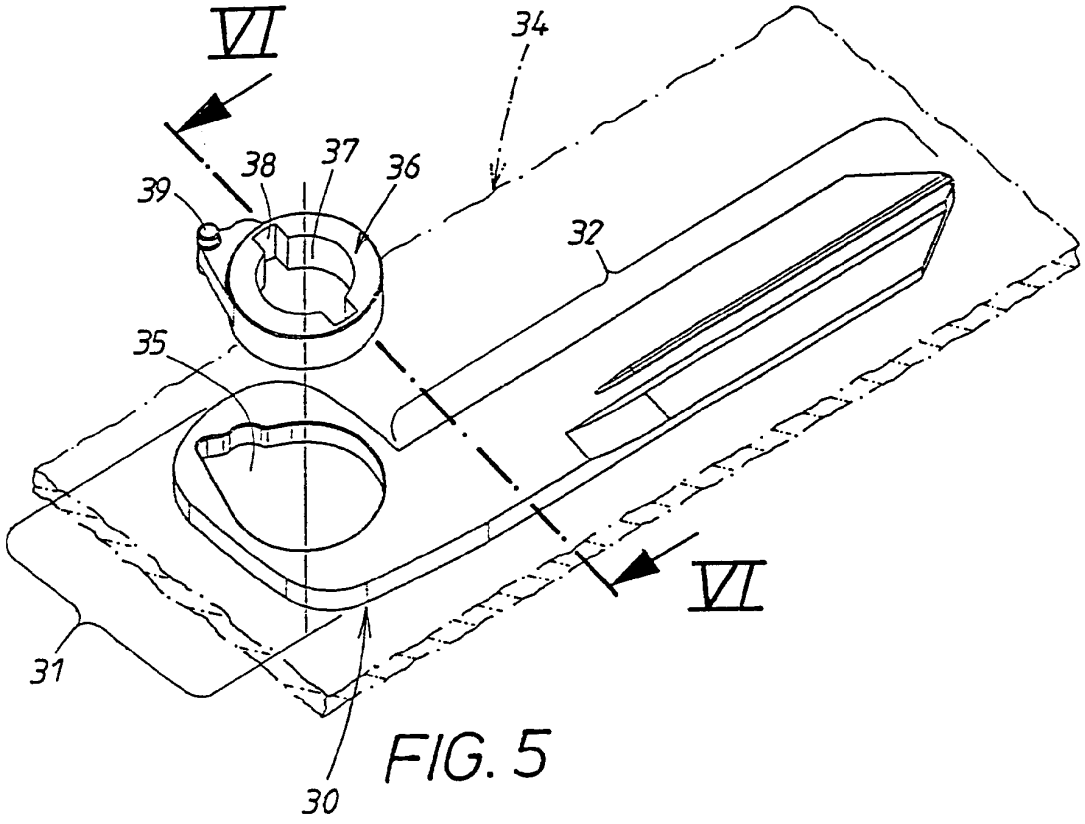


FIG. 5

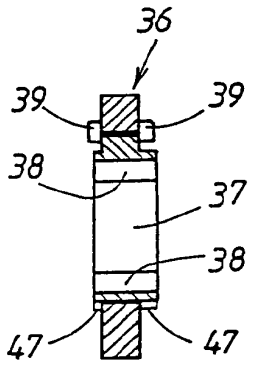


FIG. 6

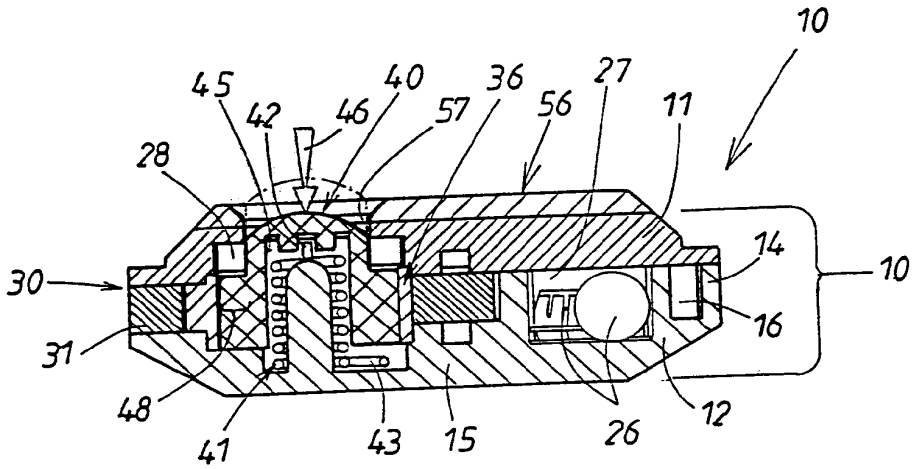

10
45
42
46
40
57
36
56
27
11
28
14
10
30
16
31
48
41
43
15
26
12

FIG. 7

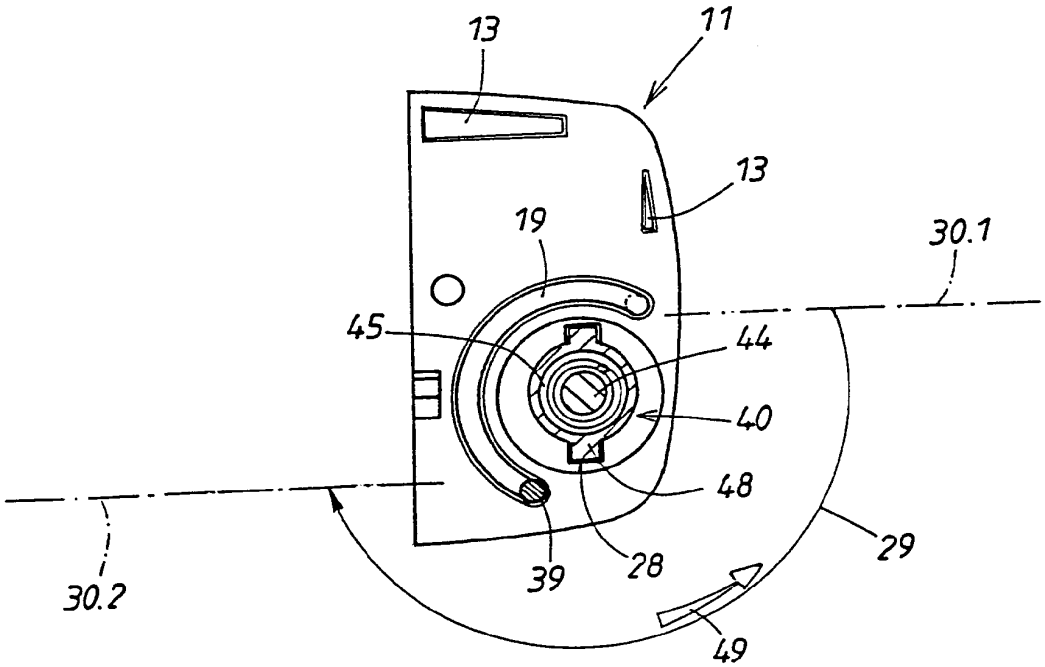

13
11
13
19
30.1
45
44
40
48
29
30.2
39
28
49

FIG. 8

INTERNATIONAL SEARCH REPORT

Int. ional Application No
PCT/EP 00/12431

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 E05B49/00 E05B19/00 E05B19/04

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 E05B A45C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 39 02 537 A (DAIMLER BENZ AG ;HUELSBECK & FUERST (DE)) 9 August 1990 (1990-08-09) cited in the application the whole document	1
A	EP 0 267 429 A (SIEMENS AG) 18 May 1988 (1988-05-18) cited in the application the whole document	1
A	US 4 726 205 A (ALLERDIST HEINZ ET AL) 23 February 1988 (1988-02-23) column 1, line 31 - line 62 column 2, line 20 - line 38; figure	1

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 March 2001	26/03/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Pieracci, A

Form PCT/ISA/210 (second sheet) (July 1992)

IPR2022-00412
Apple EX1053 Page 657

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. ional Application No
PCT/EP 00/12431

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 3902537 A	09-08-1990	NONE	
EP 0267429 A	18-05-1988	DE 3769923 D	13-06-1991
		JP 63110377 A	14-05-1988
		US 4888970 A	26-12-1989
US 4726205 A	23-02-1988	DE 3509579 A	18-09-1986
		DE 3678983 D	06-06-1991
		EP 0195195 A	24-09-1986
		JP 61229079 A	13-10-1986

IPR2022-00412
Apple EX1053 Page 658

INTERNATIONALER RECHERCHENBERICHT

Int .tionales Aktenzeichen
PCT/EP 00/12431

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 E05B49/00 E05B19/00 E05B19/04

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 E05B A45C

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE 39 02 537 A (DAIMLER BENZ AG ;HUELSBECK & FUERST (DE)) 9. August 1990 (1990-08-09) in der Anmeldung erwähnt das ganze Dokument ---	1
A	EP 0 267 429 A (SIEMENS AG) 18. Mai 1988 (1988-05-18) in der Anmeldung erwähnt das ganze Dokument ---	1
A	US 4 726 205 A (ALLERDIST HEINZ ET AL) 23. Februar 1988 (1988-02-23) Spalte 1, Zeile 31 - Zeile 62 Spalte 2, Zeile 20 - Zeile 38; Abbildung -----	1

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
16. März 2001	26/03/2001

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Pieracci, A

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

IPR2022-00412
Apple EX1053 Page 659

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/EP 00/12431

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 3902537 A	09-08-1990	KEINE	
EP 0267429 A	18-05-1988	DE 3769923 D	13-06-1991
		JP 63110377 A	14-05-1988
		US 4888970 A	26-12-1989
US 4726205 A	23-02-1988	DE 3509579 A	18-09-1986
		DE 3678983 D	06-06-1991
		EP 0195195 A	24-09-1986
		JP 61229079 A	13-10-1986

IPR2022-00412
Apple EX1053 Page 660

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 August 2001 (23.08.2001)

PCT

(10) International Publication Number
WO 01/61692 A1

(51) International Patent Classification[7]: G11B 11/00

(21) International Application Number: PCT/SG00/00029

(22) International Filing Date: 21 February 2000 (21.02.2000)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **TREK TECHNOLOGY (SINGAPORE) PTE LTD** [SG/SG]; 30 Loyang Way #07-13/14/15, Loyang Industrial Estate, Singapore 508769 (SG).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **CHENG, Chong, Seng** [SG/SG]; 129 Loyang Rise, Singapore 507472 (SG).

(74) Agent: **MCCALLUM, Graeme, David**; Lloyd Wise, Tanjong Pagar, P.O. Box 636, Singapore 910816 (SG).

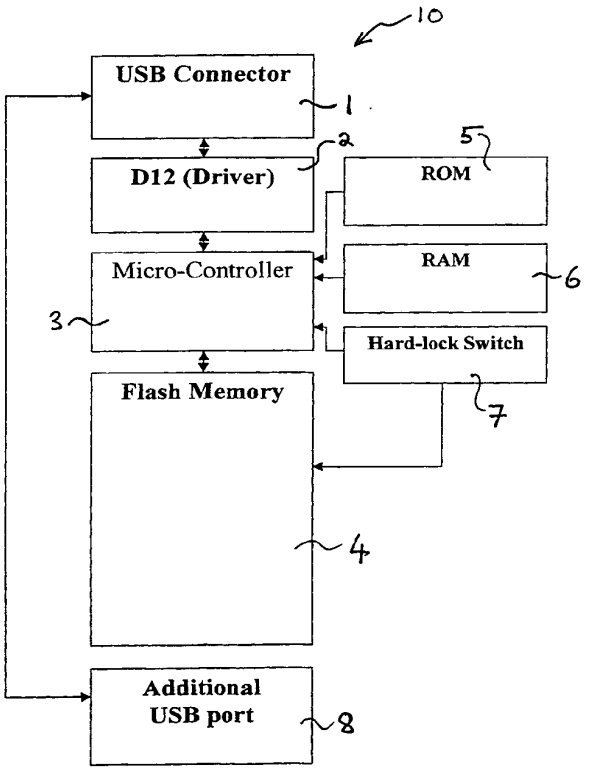
(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: A PORTABLE DATA STORAGE DEVICE



(57) Abstract: A portable data storage device (10) includes a universal serial bus (USB) coupling device (1) and an interface device (2) is coupled to the USB coupling device (1). The portable data storage device (10) also includes a memory control device (3) and a non-volatile solid-state memory device (4). The memory control device (3) is coupled between the interface device (2) and the memory device (4) to control the flow of data from the memory device (4) to the USB coupling device (1).

WO 01/61692 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

A Portable Data Storage Device

The invention relates to a portable data storage device, and in particular, a portable data storage device for a computer.

Conventional data storage devices generally fall into two categories. The first category is electronic, solid-state memory devices such as read only memory (ROM) and random access memory (RAM). These memory devices are generally fitted within the computer. They are not intended to be removable or portable so that they may be used on different computers, for example, to permit the transfer of data from one computer to another computer.

The second type of device is surface based data storage devices in which data is stored, typically, on the surface of a disk or tape. Examples of surface storage devices are magnetic disks and CD ROMs. Such data storage devices require a mechanical drive mechanism to be installed in or coupled to the computer to permit the data on the storage device to be read by the computer. In addition, such memory devices are limited by the surface area of the storage device, and the combination of the storage device and the drive mechanism for reading data from the storage device is generally bulky and/or delicate due to the moving parts that are required within the drive mechanism and/or storage device.

In accordance with the present invention, there is provided a portable data storage device comprising a coupling device for coupling to a computer serial

bus, an interface device coupled to the coupling device, a memory control device and a non-volatile solid-state memory device; the memory control device being coupled between the interface device and the memory device to control the flow of data from the memory device to the coupling device.

An advantage of the invention is that by providing a portable data storage device comprising a coupling device with an interface device, memory control device and a non-volatile solid-state memory device, it is possible to provide a portable data storage device which may be coupled to a computer having a serial bus port and which does not include moving parts or require a mechanical drive mechanism to read the data from the data storage device.

Preferably, the non-volatile solid-state memory device may be a read/write memory device, such as a flash memory device.

Preferably, where the memory device is a read/write memory device, the memory control device controls the flow of data to and from the memory device.

Typically, the data storage device further comprises a manually operated switch movable between a first position in which writing of data to the memory device is enabled, and a second position in which writing of data to the memory device is prevented.

Preferably, the memory control device may include a read only memory which stores a program to control the operation of the memory control device. Preferably, the memory control device is a micro-controller.

Typically, the interface device comprises a universal serial bus (USB) driver to convert data between a USB format and a PC format, and the coupling device comprises a USB coupling deivce.

Alternatively, the interface device comprises a driver for IEEE 1394 (Firewire) protocol, and the coupling device comprises a Firewire coupling device.

An example of a data storage device in accordance with the invention will now be described to the accompanying drawings, in which:

Figure 1 is a schematic block diagram of a portable data storage device;

Figure 2 is a flow diagram showing the initial setup of the data storage device by a software supplier;

Figure 3 is a flow diagram showing the initial setup of the data storage device by an end user; and

Figure 4 is a flow diagram showing operation of the data storage device.

Figure 1 shows a data storage device 10 which includes a USB plug 1 which is coupled to a USB interface device 2. The USB interface device 2 is coupled to a micro-controller 3 which is coupled to a flash memory 4. The micro-controller

3 includes a read only memory (ROM) 5 which stores a program to control the operation of the micro-controller 3.

The operations performed by the micro-controller 3 include comparing passwords entered by a user with a corresponding password stored in the flash memory 4 to determine whether the user is authorised to access the contents of the flash memory 4. The program stored in the ROM 5 also controls the data flow to and from the flash memory 4 and can also detect whether the computer to which the memory device 1 is coupled has installed software programs which correspond to passwords stored in the flash memory 4. The micro-controller 3 can automatically retrieve passwords from the installed software to compare with passwords stored in the flash memory to verify that a user of the computer is authorised to access and run the software. In addition, the program stored in the ROM 5 also permits the setting of a password in the flash memory by a software supplier to correspond to the password contained in software supplied to a user. Typically, the password may correspond to the serial number of the software.

The flash memory 4 is typically divided into a number of different sections or zones. Typically, the flash memory is divided into two zones and each zone has a unique password. If the data storage device 10 is supplied with packaged software, the software serial number can be set in one zone to be the password to permit a user to access and use the software. The other zone, which can be used typically for storing a user's data, may have a separate password which is set by the user. Typically, the passwords are stored in a secure location of the

flash memory in an encrypted form. The encryption, decryption, data flow control and USB protocol are all managed by the micro-controller 3.

The micro-controller 3 also includes a random access memory (RAM) 6 which is a temporary storage area to permit functioning of the micro-controller 3. In addition, a manual switch 7 is coupled between the flash memory 4 and the micro-controller 3. The manual switch 7 is movable between a first position in which a user may write data to the flash memory 4 and a second position in which data is prevented from being written to the flash memory 4.

The device 10 also includes a USB socket 8 that is coupled directly to the USB plug 1 and permits other USB devices to be coupled to the USB via the device 10. For example, if a user wishes to increase memory space, a USB plug 1 of a second memory device 10 may be connected to the USB socket 8.

Figure 2 is a flow diagram showing the set up procedure for the device 10 for a software supplier when the software supplier intends to supply the device as an authentication device for the software. Firstly, the plug 1 of the device 10 is plugged into 20 to a USB socket on a computer. After the device 10 has been plugged into the USB socket on the computer, a communication is established 21 between the computer and the device 10. The software supplier has pre-installed installation software on the computer which is run by the operator. From the pre-installed software, the operator selects password set up installation 22, in response to which the pre-installed software requests the operator to enter a password or serial number corresponding to the software

with which the device 10 is to be supplied. The password or serial number is then encrypted 26 and stored 27 in the flash memory 4.

Figure 3 is a flow diagram showing the initial set-up of a password for zone 2 of the flash memory 4 by an end user. The device 10 is typically supplied with driver software that is loaded by the user onto the computer prior to set-up of the device. To set-up the password for zone 2 the user plugs in 20 the device 10 into a USB port on the computer and communication 21 is established between the computer and the device 10. The user then runs the driver software and the driver software enters a password installation set-up mode 23 for zone 2. The user then enters 28 a password that they wish to use to prevent unauthorised access to zone 2 of the flash memory 4. The password entered is then encrypted 29 and stored 30 in the flash memory 4.

After an end user has performed the initial password set up procedure described above and shown in Figure 3, when a user plugs in 20 the device 10 to a USB port on a computer, the computer will establish a communication 21 with the device 10 and firstly, checks 33 an installation status flag stored in the flash memory 4 (see Figure 4). If the status flag is "Y", the device 10 outputs 34 an "OK" flag to the computer. The micro-controller 3 the instructs the computer to issue a request 35 to the user to select the zone they wish to enter. If the status flag is "N", the device does not output an "OK" flag to the computer, and goes straight to step 35. In response to the request 35 for zone selection, the user selects 36 either zone 1 or zone 2.

If zone 1 is selected, the device 10 assumes that the user wishes to install software on the computer which is stored in the flash memory 4 and requests 37 the appropriate password for confirmation that the user is authorised to install the software. The micro-controller 3 receives the password entered by the user, retrieves the zone 1 password stored in the flash memory 4, decrypts the zone 1 password and compares it with the password entered by the user to authenticate 38 whether the user is authorised to install the software. If the passwords do not match, the device 10 prompts the computer to request 37 the user to enter the password again.

If the password entered by the user matches the password stored in the flash memory 4, the micro-controller 3 starts 39 the software installation from the flash memory 4 to the computer. In order to install software, the computer sends 40 a read/write command in USB format to the micro-controller 3 for data, the micro-controller 3 retrieves the requested data from the flash memory 4 and sends 41 the data to the driver 2. The driver 2 converts 42 the data to PC format and outputs the data to the computer through the USB plug 1. The micro-controller 3 then checks 43 whether the software installation is complete. If the operation is not complete, the operation returns to step 40. If the installation of the software is complete, the status flag stored in the flash memory 4 is changed to "Y" and the device 10 may then be removed 45 from the USB socket on the computer.

If a user selects zone 2, the micro-controller 3 sends a command to the computer to request 46 the user to enter the password for zone 2. When the

user enters the password, the computer sends the password to the micro-controller 3. The micro-controller 3 retrieves the password for zone 2 from the flash memory 4, decrypts 47 the password and compares it with the password entered by the user. If the password entered by the user is incorrect, the operation returns to step 46 and the computer requests 46 the user for the password again.

If the password entered by the user is correct, the user has access to zone 2 of the flash memory 4 to read data from the flash memory 4 and to write data to the flash memory 4. However, data can only be written to the flash memory 4 if the manual switch 7 is in the position to permit data to be written to the flash memory 4. In order to read or write data from or to the flash memory 4 a read or write command is sent 48 by the computer in USB format to the micro-controller 3. In response to the read or write command the micro-controller 3 either retrieves 49 data from the flash memory 4 and sends it to the driver 2 for conversion 50 to PC format and then to be output to the computer or receives data from the driver to write it to the flash memory 4.

The micro-controller 3 then determines 51 whether the read or write operation is complete. If the operation is not complete it returns to step 48. If the operation is complete the operation terminates 52.

The device 10 described above is for coupling to a universal serial bus (USB). However, the plug 1, the interface device 2 and socket 8 could be for use with any appropriate computer serial bus. For example, the device 10 could be

modified for use with IEEE 1394 (Firewire) protocol by substituting the USB plug 1, USB interface device 2 and socket 8 with a Firewire protocol compatible plug, interface device and socket respectively.

An advantage of the device 10 described above is that it provides a portable data storage device for a computer which does not require a mechanical operated reading/writing device. In addition, the device 10 has no moving parts. This enables to data storage device 10 to be more compact than conventional portable data storage devices.

CLAIMS

1. A portable data storage device comprising a coupling device for coupling to a computer serial bus, an interface device coupled to the coupling device, a memory control device and a non-volatile solid-state memory device; the memory control device being coupled between the interface device and the memory device to control the flow of data from the memory device to the coupling device.

2. A device according to claim 1, wherein the non-volatile solid-state memory device is a read/write memory device.

3. A device according to claim 2, wherein the read/write memory device is a flash memory device.

4. A device according to claim 2 or claim 3, wherein the memory control device controls the flow of data to and from the memory device.

5. A device according to any of claims 2 to 4, further comprising a manually operated switch movable between a first position in which writing of data to the memory device is enabled, and a second position in which writing of data to the memory device is prevented.

6. A device according to any of the preceding claims, wherein the memory control device comprises a micro-controller.

7. A device acccrding to any of the preceding claims, wherein the coupling device comprises a ι niversal serial bus coupling device and the interface device comprises a USB driver.

8. A device according to any of the preceding claims, wherein the coupling device comprises an IEEE 1394 (Firewire) protocol coupling device and the interface device is a Firewire protocol driver.

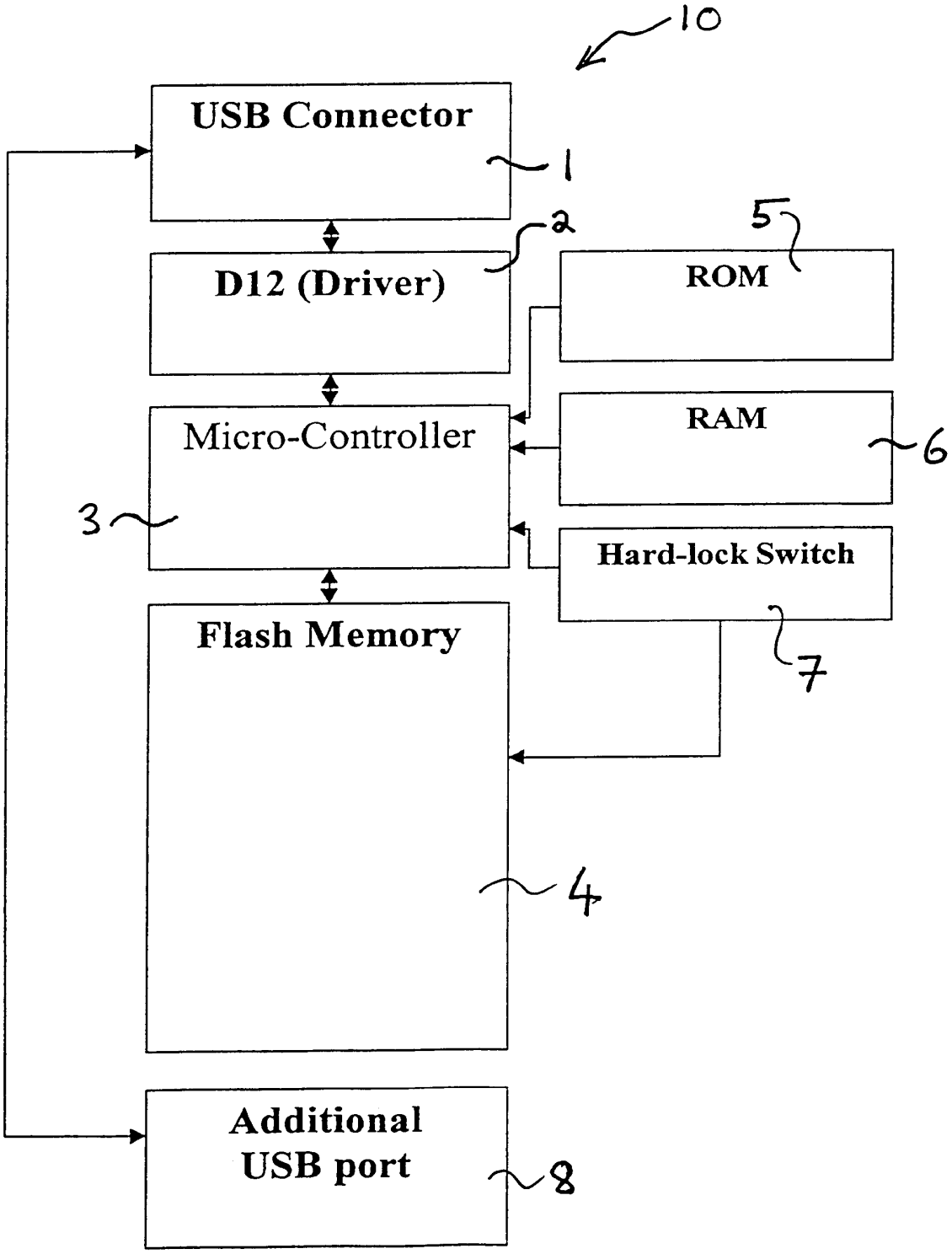

10
USB Connector
1
2
D12 (Driver)
5
ROM
Micro-Controller
RAM
6
3
Hard-lock Switch
7
Flash Memory
4
Additional
USB port
8

Figure 1

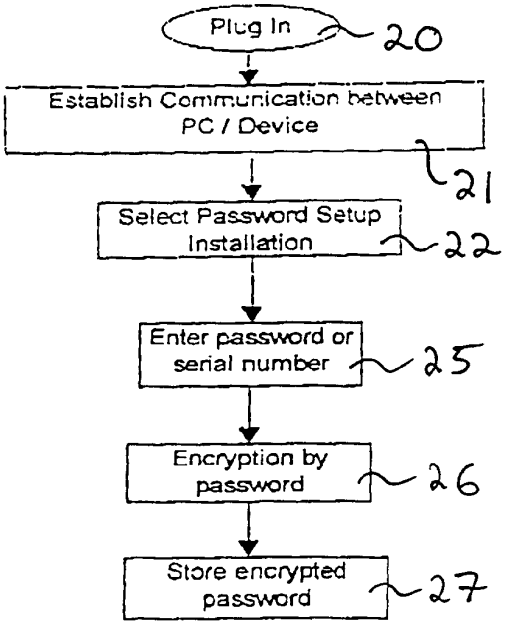


Figure 2

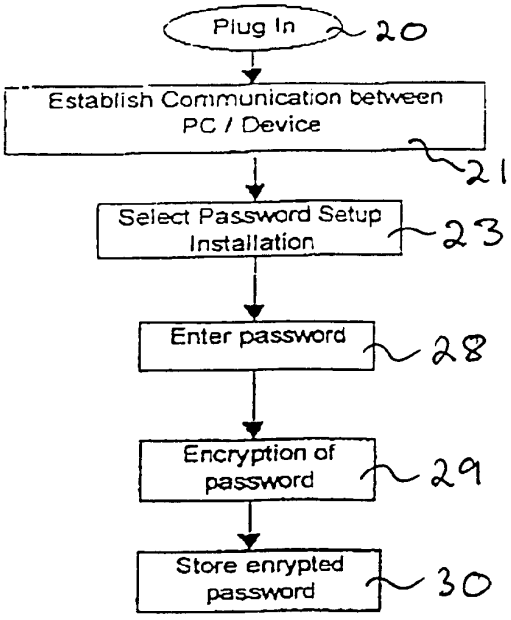


Figure 3

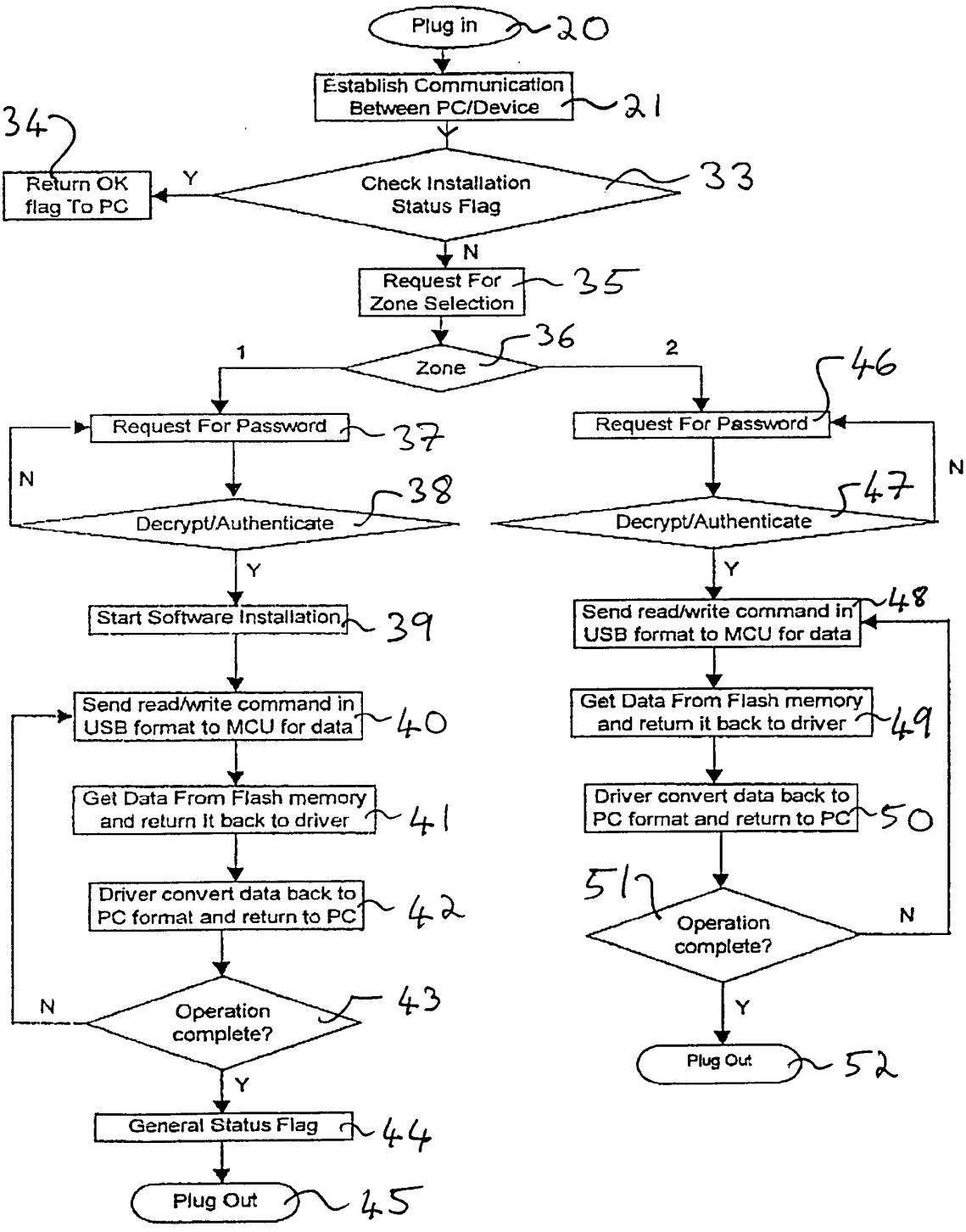

Plug in
20
Establish Communication Between PC/Device
21
34
Return OK flag To PC
Y
Check Installation Status Flag
33
N
Request For Zone Selection
35
Zone
36
1
2
Request For Password
37
N
Decrypt/Authenticate
38
Y
Start Software Installation
39
Send read/write command in USB format to MCU for data
40
Get Data From Flash memory and return it back to driver
41
Driver convert data back to PC format and return to PC
42
N
Operation complete?
43
Y
General Status Flag
44
Plug Out
45
46
Request For Password
N
47
Decrypt/Authenticate
Y
48
Send read/write command in USB format to MCU for data
Get Data From Flash memory and return it back to driver
49
Driver convert data back to PC format and return to PC
50
51
Operation complete?
N
Y
Plug Out
52

Figure 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG 00/00029

CLASSIFICATION OF SUBJECT MATTER

IPC[7]: G11B 11/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC[7]: G11B 11/00, 02,05

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

G06F 3/00, 12/00, 12/06

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6016530 A (AUCLAIR et al.) 18 January 2000 (18.01.00)	1
P,A	US 6058441 A (SHU) 2 May 2000 (02.05.00)	1
A	US 5760986 A (MOREHOUSE et al.) 2 June 1998 (02.06.98)	1

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
„A" document defining the general state of the art which is not considered to be of particular relevance
„E" earlier application or patent but published on or after the international filing date
„L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
„O" document referring to an oral disclosure, use, exhibition or other means
„P" document published prior to the international filing date but later than the priority date claimed

„T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
„X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
„Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
„&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 March 2001 (24.03.2001)	12 April 2001 (12.04.2001)

Name and mailing adress of the ISA/AT	Authorized officer
Austrian Patent Office Kohlmarkt 8-10; A-1014 Vienna	GRÖSSING
Facsimile No. 1/53424/535	Telephone No. 1/53424/386

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/SG 00/00029

Patent document cited in search report			Publication date	Patent family member(s)			Publication date
US	A	5760986	0[illegible]-06-1998	EP	A1	614564	14-09-1994
				EP	A4	614564	19-07-1995
				US	A	5379171	03-01-1995
				WO	A1	9306594	01-04-1993
				US	A	5835303	10-11-1998
				US	A	5579189	26-11-1996
				US	A	5592349	07-01-1997
				US	A	5694267	02-12-1997
				US	A	5867340	02-02-1999
US	A	6016530	18-01-2000	US	A	5778418	07-07-1998
US	A	6058441	02-05-2000			none	

IPR2022-00412
Apple EX1053 Page 678

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
22. November 2001 (22.11.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/88693 A2

(51) Internationale Patentklassifikation[7]: G06F 7/72

(21) Internationales Aktenzeichen: PCT/EP01/05532

(22) Internationales Anmeldedatum:
15. Mai 2001 (15.05.2001)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
100 24 325.8 17. Mai 2000 (17.05.2000) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **GIESECKE & DEVRIENT GMBH** [DE/DE]; Prinzregentenstrasse 159, 81677 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: **SEYSEN, Martin** [DE/DE]; Schleissheimer Strasse 339, 80809 München (DE).

(74) Anwalt: **KLUNKER, SCHMITT-NILSON, HIRSCH**; Winzererstrasse 106, 80797 München (DE).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Bestimmungsstaaten *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:
— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

WO 01/88693 A2

(54) **Title:** CRYPTOGRAPHIC METHOD AND CRYPTOGRAPHIC DEVICE

(54) **Bezeichnung:** KRYPTOGRAPHISCHES VERFAHREN UND KRYPTOGRAPHISCHE VORRICHTUNG

(57) **Abstract:** The invention relates to a cryptographic method comprising at least one arithmetic step which contains a modular exponentiation E, according to the equation $E=x^d(\mathrm{mod}\ p.q)$, comprising a first prime factor p, a second prime factor q, an exponent d and a number x. According to said method, the modular exponentiation E is calculated according to the Chinese Remainder Theorem.

(57) **Zusammenfassung:** Die Erfindung betrifft ein kryptographisches Verfahren mit mindestens einem eine modulare Exponentiation E gemäss $E=x^d(\mathrm{mod}\ p \cdot q)$ enthaltenden Rechenschritt mit einem ersten Primfaktor p, einem zweiten Primfaktor q, einem Exponenten d und einer Zahl x, wobei die modulare Exponentiation E gemäss dem Chinesischen Restwertsatz berechnet wird.

IPR2022-00412
Apple EX1053 Page 679

Kryptographisches Verfahren und kryptographische Vorrichtung

Kryptographische Verfahren in Gestalt von Verschlüsselungs- und Signaturverfahren erfreuen sich insbesondere durch die steigende Bedeutung des elektronischen Geschäftsverkehres einer stetig wachsenden Verbreitung. Sie werden in der Regel mittels elektronischer Vorrichtungen implementiert, die beispielsweise einen programmierbaren universellen Microkontroller oder auch eine spezialisierte elektronische Schaltung etwa in Gestalt eines ASIC beinhalten können. Eine besonders interessante Form kryptographischer Vorrichtungen ist die Chipkarte, da sich in ihr bei zweckdienlicher technischer Ausgestaltung geheime Schlüsseldaten gegen unbefugten Zugriff schützen lassen. Ein ständiges Bemühen gilt dabei sowohl der Verbesserung der Ausführungsgeschwindigkeit der kryptographischen Verfahren als auch deren Sicherung gegen alle denkbaren Arten von Angriffen. Die Erfindung eignet sich insbesondere für den Einsatz im Zusammenhang mit Chipkarten, ist aber in keiner Weise darauf beschränkt. Sie ist vielmehr im Zusammenhang mit allen Arten von kryptographischen Vorrichtungen implementierbar.

Bei einer Reihe bekannter kryptographischer Verfahren ist es erforderlich, eine modulare Exponentiation gemäß der Gleichung

$$E = x^d \pmod N = x^d \pmod{p \cdot q} \qquad (1)$$

durchzuführen, wobei p und q Primzahlen sind. Ein besonders bedeutendes kryptographisches Verfahren, welches einen modularen Exponentiationsschritt beinhaltet, ist das beispielsweise aus Alfred J. Menezes, Paul C. van Oorschot und Scott A. Vanstone, "Handbook of Applied Cryptography", Boca Raton: CRC Press, 1997, Seiten 285 bis 291, bekannte RSA-Verfahren. Die Verwendung der modularen Exponentiation ist jedoch nicht auf das RSA-Verfahren beschränkt, sondern umfaßt beispielsweise auch aus Menezes et al., a.a.O., Seiten 438 bis 442, bekannte Rabin-Signaturen und das aus Mene-

IPR2022-00412
Apple EX1053 Page 680

zes et al., a.a.O., Seite 408 bis 410, bekannte Fiat-Shamir'sche Identifikationsschema.

Die Sicherheit von kryptographischen Verfahren, die die modulare Exponentiation einbeziehen, ist regelmäßig abhängig von der Schwierigkeit, die Zahl N aus Gleichung (1) in ihre Primfaktoren p und q zerlegen zu können. Dieses Problem ist nur für hinreichend große Werte N von ausreichender Komplexität, so daß einerseits N möglichst groß gewählt werden sollte. Der Rechenaufwand zur Berechnung von Werten mittels modularer Exponentiation gemäß Gleichung (1) steigt andererseits monoton mit der Größenordnung von N, so daß es unter dem Gesichtspunkt der praktischen Anwendbarkeit wünschenswert wäre, trotz großer Werte von N den Rechenzeitaufwand auf akzeptable Werte beschränken zu können.

Es ist bekannt, durch Anwendung des sog. "Chinesischen Restwertsatzes" die Rechengeschwindigkeit um einen Faktor 4 erhöhen zu können, wodurch beispielsweise bei gleicher Rechenzeit größere Werte N zugelassen werden können. Statt unmittelbar die Gleichung (1) auszuwerten, wird eine Umformung vorgenommen gemäß

$$E = x^d \pmod{p \cdot q} = aE_1 + bE_2 \pmod{N} \qquad (2)$$

mit

$$E_1 = x^d \pmod{p} \qquad (3)$$

$$E_2 = x^d \pmod{q} \qquad (4)$$

Eine Folge der Anwendung des Chinesischen Restwertsatzes besteht darin, daß die modulare Exponentiation nicht mehr modulo N, also modulo derjenigen Zahl, die ihre eigene Primfaktorzerlegung noch in sich verbirgt, sondern nacheinander in einem ersten Teilschritt modulo p und in einem zweiten Teilschritt modulo q erfolgt, d.h. die Kenntnis der geheimzuhaltenden

Primfaktorzerlegung $n = p \cdot q$ wird bei dieser Rechenvorschrift vorausgesetzt und führt zu einer Aufteilung des Gesamtrechenprozesses in einen ersten Rechenschritt (3), in den der erste Primfaktor wesentlich eingeht, und einen zweiten Rechenschritt (4), in den der zweite Primfaktor wesentlich eingeht. Der Vorteil hierbei liegt darin, daß der Exponent d in Gleichung (1) modulo $\phi(p \cdot q)$ definiert sein muß, wohingegen die Exponenten in Gleichung (2) lediglich modulo $\phi(p)$ bzw. $\phi(q)$ definiert sein müssen, wobei mit ϕ die Euler'sche Funktion notiert ist.

Interessanterweise ist nun in der letzten Zeit ein Angriffsschema auf solche kryptographischen Verfahren, die die modulare Exponentiation nutzen, bekannt geworden, bei dem durch einen geeigneten artifiziellen Eingriff in den ansonsten störungsfreien Rechenablauf aus dem fehlerhaften Ergebnis einer gestörten modularen Exponentiation die Information über die Primfaktorzerlegung von N zurückgewonnen werden kann, sofern die konkrete Implementation von dem Chinesischen Restwertsatz gemäß den Gleichungen (2) bis (4) Gebrauch macht. Dieser als "Bellcore-Angriff" bekannte Versuch ist beispielsweise in Dan Boneh, Richard A. DeMillo und Richard J. Lipton: "On the importance of checking Cryptographic Protocols for Faults", Advances in Cryptology -EUROCRYPT, 97, Lecture Notes in Computer Science 1233, Berlin: Springer, 1997 beschrieben. Eine Verschlüsselungseinrichtung wird durch physikalische Eingriffe wie beispielsweise Übertaktung, zu hohe Betriebsspannung oder Bestrahlung manipuliert, so daß mit einer gewissen, nicht zu großen Wahrscheinlichkeit Rechenfehler bei der Ausführung der modularen Exponentiation nach dem Chinesischen Restwertsatz auftreten. Wenn ein Rechenfehler nur bei einem der beiden Terme in Gleichung (2) auftritt, können die beiden Primfaktoren p und q aus dem fehlerbehafteten Exponentiationsergebnis rekonstruiert werden.

IPR2022-00412
Apple EX1053 Page 682

Die aus dieser Verletzlichkeit der mittels des Chinesischen Restwertsatzes implementierten modularen Exponentiation zu ziehende Konsequenz besteht darin, das Ergebnis des Rechenvorganges zuerst auf seine Korrektheit zu prüfen, bevor es weiterverarbeitet, insbesondere aber bevor es in irgend einer Form, etwa in Gestalt einer Signatur, ausgegeben wird.

Ein triviales Gegenmittel gegen den "Bellcore-Angriff" besteht darin, diese Korrektheitsprüfung dadurch zu bewerkstelligen, indem der Rechenvorgang mindestens einmal wiederholt wird. Bei zufälligen Rechenfehlern kann davon ausgegangen werden, daß das Ergebnis des ersten Rechenganges von demjenigen der Kontrollrechengänge abweicht. Der wesentliche Nachteil dieses Ansatzes besteht darin, daß sich die Rechenzeit bereits bei einer Kontrollrechnung verdoppelt.

Aus der Druckschrift WO-A1-98/52319 ist insbesondere ein Verfahren zum Schutz von eine modulare Exponentiation nach dem Chinesischen Restwertsatz ausführenden Rechenoperationen gegen den "Bellcore-Angriff" bekannt. Dabei wird eine geheime ganz Zahl j beispielsweise im Bereich $[0, 2^k-1]$ mit $16 \leq k \leq 32$ ausgewählt. Sodann werden folgende Ausdrücke berechnet:

$$v_1 = x \pmod{j \cdot q} \tag{5}$$

$$v_2 = x \pmod{j \cdot q} \tag{6}$$

$$d_1 = d \pmod{\phi(j \cdot p)} \tag{7}$$

$$d_2 = d \pmod{\phi(j \cdot q)} \tag{8}$$

$$w_1 = v_1^{d1} \pmod{j \cdot p} \tag{9}$$

$$w_2 = v_2^{d2} \pmod{j \cdot q} \tag{10}$$

Sodann wird geprüft, ob gilt:

$$w_1 = w_2 \pmod{j} \tag{11}$$

Kann der Ausdrucke (11) verifiziert werden, so werden bei dem bekannten Verfahren folgende Ausdrücke berechnet:

$$y_1 = w_1 \pmod{p} \tag{12}$$

$$y_2 = w_2 \pmod{q} \tag{13}$$

woraus dann mittels des Chinesischen Restwertsatzes der Wert für

$$E = x^d \pmod{N} \tag{14}$$

ermittelt werden kann.

Dieses bekannte Verfahren weist gegenüber einfachen Kontrollrechengängen den Vorteil auf, daß der zusätzliche Rechenzeitaufwand wesentlich geringer ist.

Bei diesem Verfahren müssen beide Primzahlen p und q mit demselben Faktor d multipliziert werden. In der Druckschrift WO-A1-98/52319 ist ein zweites Verfahren beschrieben, welches es erlaubt, die Primzahlen p und q mit verschiedenen Faktoren r und s zu multiplizieren. Hierbei sind jedoch für die Kontrollrechnung zwei weitere Exponentiationen möglich.

Aufgabe der Erfindung ist es, ein kryptographisches Verfahren bzw. eine kryptographische Vorrichtung anzugeben, bei dem bzw. bei der unter Beibehaltung oder Erhöhung der Sicherheit Rechenoperationen oder Rechenzeit eingespart werden kann.

Diese Aufgabe wird erfindungsgemäß gelöst durch ein kryptographisches Verfahren mit den in Anspruch 1 oder 2 angegebenen Merkmalen als auch durch eine kryptographische Vorrichtung mit den in Anspruch 13 oder 14 angegebenen Merkmalen.

IPR2022-00412
Apple EX1053 Page 684

Den abhängigen Ansprüchen 3 bis 12 sowie 15 bis 24 sind vorteilhafte Weiterbildungen entnehmbar.

Wie weiter unten erwähnt wird, ist es auf bestimmten Rechenwerken vorteilhaft, wenn ein Modulus bei der modularen Exponentiation viele führende binäre Einsen besitzt, so daß verschiedene Faktoren r und s hier einen gewissen Vorteil bedeuten. Ferner gibt es für die modulare Exponentiation optimierte Rechenwerke, wobei aber allein der Datentransfer von der Zentraleinheit in das optimierte Rechenwerk für die Exponentiation einen beträchtlichen Verwaltungsaufwand verursacht. Die vorliegende Erfindung spart gegenüber dem oben beschriebenen Verfahren bei verschiedenen Faktoren r und s eine Exponentiation ein.

Erfindungsgemäß werden zwei ganze Zahlen r und s beispielsweise im Bereich $[0, 2^k\text{-}1]$ mit $16 \leq k \leq 32$ ausgewählt, so daß d teilerfremd zu $\phi(kgV(r,s))$ ist, wobei kgV(r,s) das kleinste gemeinsame Vielfache von r und s angibt, und $\phi()$ die Euler'sche Funktion darstellt. Sodann werden folgende Ausdrükke berechnet:

$$x_1 = x \pmod{p \cdot r} \tag{15}$$

$$x_2 = x \pmod{q \cdot s} \tag{16}$$

$$d\_1 = d \pmod{\phi(p \cdot r)} \tag{15}$$

$$d\_2 = d \pmod{\phi(q \cdot s)} \tag{16}$$

$$z_1 = x_1^{d\_1} \pmod{p \cdot r} \tag{15}$$

$$z_2 = x_2^{d\_2} \pmod{q \cdot s} \tag{16}$$

Jetzt gilt $z_1 = x^d \pmod{p \cdot r}$ und $z_2 = x^d \pmod{q \cdot s}$. Nach dem Chinesischen Restwertsatz läßt sich aus z_1 und z_2 leicht eine Zahl z berechnen mit

$$z = z_1 \pmod{p \cdot r} \; ; \; z = z_2 \pmod{q \cdot s} \; ; \; z = x^d \pmod{p \cdot q \cdot kgV(r,s)} \quad (17)$$

Die Zahlen r und s müssen erfindungsgemäß so gewählt werden, daß d teilerfremd ist zu $\phi(kgV(r,s))$. Unter diesen Umständen läßt sich mit Hilfe des erweiterten Euklid'schen Algorithmus leicht eine natürliche Zahl e finden mit

$$e \cdot d = 1 \pmod{\phi(kgV(r,s))} \quad (18)$$

Mit Hilfe von Z und e wird die Zahl C wie folgt berechnet:

$$C = z^e \pmod{kgV(r,s)} \quad (19)$$

Nach dem Satz von Euler gilt:

$$C = x^{d \cdot e} = x \pmod{kgV(r,s)} \quad (20)$$

Durch Vergleich der beiden Werte C und x modulo kgV(r,s) läßt sich ein Fehler mit hoher Wahrscheinlichkeit feststellen. Wenn $C \neq x \pmod{kgV(r,s)}$ festgestellt wird, ist das Ergebnis der modularen Exponentiation als fehlerbehaftet anzusehen und zu verwerfen.

Bei RSA-Verfahren (ebenso wie beim Rabin'schen Signaturverfahren) ist zur Erzeugung einer digitalen Signatur oder zur Entschlüsselung eine modulare Exponentiation durchzuführen, wobei der Modulus p·q und Exponent d nur vom privaten Schlüssel abhängen. Infolgedessen können die Zahlen d, e, r und s einmal beim Einbringen des privaten Schlüssel berechnet und zur Wiederverwendung abgespeichert werden.

In einer Variante der Erfindung werden ebenfalls zwei ganze Zahlen r und s beispielsweise im Bereich $[0, 2^k\text{-}1]$ mit $16 \leq k \leq 32$ ausgewählt. Auf einem binären Rechenwerk wird empfohlen, daß die Zahlen r und s beide ungerade sind. Außerdem werden zwei feste, nicht von x abhängige Zahlen b_1 und b_2 im Intervall [1,...,r-1] bzw. [1,...,s-1] und teilerfremd zu r bzw. s gewählt. Falls r und s nicht teilerfremd sind, müssen b_1 und b_2 die zusätzliche Bedin-

IPR2022-00412
Apple EX1053 Page 686

gung $b_1 = b_2 \pmod{ggT(r,s)}$ erfüllen, wobei ggT(r,s) den größten gemeinsamen Teiler von r und s bezeichnet.

Nach dem Chinesischen Restsatz wird zunächst eine Zahl x_1 berechnet mit

$$x_1 = x \pmod{p}, \quad x_1 = b_1 \pmod{r} \tag{21}$$

Ebenso wird eine Zahl x_2 berechnet mit

$$x_2 = x \pmod{q}, \quad x_2 = b_2 \pmod{s} \tag{22}$$

Sodann werden folgende Ausdrücke berechnet:

$$d\_1 = d \pmod{\phi(p)} \tag{23}$$

$$d\_2 = d \pmod{\phi(q)} \tag{24}$$

$$z_1 = x_1^{d\_1} \pmod{p \cdot r} \tag{25}$$

$$z_2 = x_2^{d\_2} \pmod{q \cdot s} \tag{26}$$

$$C_1 = b_1^{d\_1} \pmod{\cdot r} \tag{27}$$

$$C_2 = b_2^{d\_2} \pmod{\cdot s} \tag{28}$$

Zur Einsparung von Rechenzeit können die Exponenten d_1 und d_2 in (27) bzw. (28) vor der Durchführung der Exponentiation modulo $\phi(r)$ bzw. $\phi(s)$ reduziert werden.

Aus (23) und (25) folgt

$$z_1 = x^d \pmod{p} \tag{29}$$

Aus (24) und (26) folgt

$$z_2 = x^d \pmod{q}. \tag{30}$$

Nach dem Chinesischen Restwertsatz läßt sich aus z_1 und z_2 leicht eine Zahl z berechnen mit

$$z = z_1 \pmod{p \cdot r}\ ;\ z = z_2 \pmod{q \cdot s}\ ; \tag{31}$$

Selbst wenn r und s nicht teilerfremd sind, existiert eine solche Zahl z wegen $z_1 = C_1 = b_1^{d\_1} = b_2^{d\_2} = C_2 = z_2 \pmod{ggT(r,s)}$. Da p und q teilerfremd sind, folgt aus (29), (30) und (31):

$$z = x^d \pmod{p \cdot q}. \tag{32}$$

so daß sich die gesuchte Zahl z leicht aus den oben berechneten Werten ermitteln läßt.

Aus (21), (25) und (27) folgt

$$z_1 = C_1 \pmod{r} \tag{33}$$

Aus (22), (26) und (28) folgt

$$z_2 = C_2 \pmod{s} \ . \tag{34}$$

Durch Prüfung der Bedingungen (33) und (34) läßt sich ein Fehler mit hoher Wahrscheinlichkeit feststellen. Wenn eine der Bedingungen (33) oder (34) verletzt wird, ist das Ergebnis der modularen Exponentiation als fehlerbehaftet anzusehen und zu verwerfen.

Im Gegensatz zu dem Verfahren in Patentanspruch 8 der Druckschrift WO-A1-98/52319 sind die Zahlen b_1 und b_2 in der hier vorgestellten Variante des Verfahrens nicht von der Basis x abhängig. Typischerweise wird bei der Anwendung des RSA-Verfahrens oder des Rabin'schen Signaturverfahrens ein privater Schlüssel einmal in ein kryptographisches Gerät, z. B: in eine Chipkarte eingebracht, und anschließend mehrmals verwendet. Hierbei ist bei der in diesen Verfahren angewendeten modularen Exponentiation der Exponent d sowie der Modulus $p \cdot q$ jeweils ein fester Bestandteil des privaten Schlüssels. Infolgedessen müssen die Werte C_1 und C_2 nur einmal beim Einbringen des Schlüssels in das kryptographische Gerät berechnet werden, und können dann anschließend in dem Gerät abgespeichert werden. Das

IPR2022-00412
Apple EX1053 Page 688

Abspeichern dieser Werte spart ggü. dem in der Druckschrift WO-A1-98/52319 vorgestellten Verfahren zwei modulare Exponentiationen.

Eine kryptographische Vorrichtung, beispielsweise eine Chipkarte, mit einer Zusatzhardware für die Beschleunigung der modularen Arithmetik enthält bei üblichen Ausführungsformen schnelle Addier- und/oder Multiplizierereinheiten, während die bei der modularen Reduktion erforderliche Division durch eine lange Zahl nach üblichen Standardverfahren durchgeführt werden muß, wie sie beispielsweise aus Donald Knuth: "The Art of Computer Programming", Volume 2: Seminumerical Algorithms, 2. Ed., Addison-Wesley, 1981, bekannt sind. Eines von mehreren bekannten Verfahren zur Vereinfachung der Divisionsoperation besteht darin, den Modulus p vor der Exponentiation mit einer Zahl r zu multiplizieren, so daß die Binärdarstellung des Produktes p·r möglichst viele Einsen enthält; siehe beispielsweise Menezes et al. a.a.O., Seiten 598 bis 599. Die Division durch eine Zahl mit möglichst vielen führenden Einsen ist erheblich einfacher als die Division durch eine allgemeine Zahl.

Der Multiplikator r wird erfindungsgemäß so gewählt, daß d teilerfremd zu $\phi(r)$ ist. Bei der o.g. Variante der Erfindung ist diese Teilerfremdheit nicht erforderlich. Für jeden Modulus p gibt es einen von der jeweiligen technischen Implementierung der Division abhängigen optimalen Multiplikator r_{opt}. Falls der gewählte Wert von r geringfügig kleiner als das Optimum ist, enthält das Produkt p·r immer noch genügend viele führende Einsen, um die Division einfach gestalten zu können. Mit hoher Wahrscheinlichkeit ist die Zahl d teilerfremd zu mindestens einem der Werte $\phi(r_{opt}-i)$, wobei $i = 1, ..., k$, wobei k eine von der Implementation abhängige kleine Zahl ist.

IPR2022-00412
Apple EX1053 Page 689

Wenn dies nicht der Fall ist, ersetze man r durch $2^i \cdot r$, wobei 2^i eine von der Implementierung abhängige geeignete Zweierpotenz ist.

Dieselben Substitutionen sind entsprechend auch auf den zweiten Primfaktor q anwendbar. Da die Multiplikatoren r (für p) und s (für q) unabhängig voneinander gewählt werden können, ist für den Multiplikator s ebenfalls eine entsprechende Wahl möglich.

IPR2022-00412
Apple EX1053 Page 690

Patentansprüche

1. Kryptographisches Verfahren,

a) mit mindestens einem eine modulare Exponentiation E

$E = x^d \pmod{p \cdot q}$

enthaltenden Rechenschritt mit einem ersten Primfaktor p, einem zweiten Primfaktor q, einem Exponenten d und einer Basis x, wobei

b) zur Durchführung der modularen Exponentiation zwei natürliche Zahlen r und s gewählt werden mit der Bedingung , daß d teilerfremd ist zu $\phi(kgV(r,s))$ und wobei die folgenden Rechenschritte durchgeführt werden:

$$x_1 = x \pmod{p \cdot r}$$

$$x_2 = x \pmod{q \cdot s}$$

$$d\_1 = d \pmod{\phi(p \cdot r)}$$

$$d\_2 = d \pmod{\phi(q \cdot s)}$$

$$z_1 = x_1^{d\_1} \pmod{p \cdot r}$$

$$z_2 = x_2^{d\_2} \pmod{q \cdot s},$$

und wobei $\phi(.)$ die Euler'sche Funktion und kgV(r,s) das kleinste gemeinsame Vielfache von r und s darstellt,

c) anschließend nach dem Chinesischen Restwertsatz aus z_1 und z_2 eine Zahl z berechnet wird mit $z = z_1 \pmod{p \cdot r}$; $z = z_2 \pmod{q \cdot s}$;

d) das Ergebnis E der Exponentiation durch Reduktion von z modulo $p \cdot q$ berechnet wird

e) die vorher berechnete Zahl z und damit das Ergebnis E in einem Prüfschritt auf Rechenfehler geprüft wird,

f) der Prüfschritt folgende Rechenoperationen beinhaltet:

IPR2022-00412
Apple EX1053 Page 691

f1) Berechnen der kleinstmöglichen natürlichen Zahl e mit der Eigenschaft $e \cdot d = 1 \pmod{\phi(kgV(r,s))}$ mit Hilfe des erweiterten Euklids'schen Algorithmus

f2) Berechnen des Wertes $C = z^e \pmod{kgV(r,s)}$

f3) Vergleich der Werte x und C modulo kgV(r,s), wobei das Ergebnis der modularen Exponentiation E als fehlerhaft verworfen wird, wenn $x \neq C \pmod{kgV(r,s)}$.

2. Kryptographisches Verfahren,

a) mit mindestens einer eine modulare Exponentiation E

$E = x^d \pmod{p \cdot q}$

enthaltenden Rechenschritt mit einem ersten Primfaktor p, einem zweiten Primfaktor q, einem Exponenten d und einer Basis x, wobei

b) zur Durchführung der modularen Exponentiation zwei natürliche Zahlen r und s , sowie zwei Zahlen b_1 und b_2 im Intervall [1,...,r-1] bzw. [1,...,s-1] und teilerfremd zu r bzw. s gewählt werden, und wobei b_1 und b_2 die Bedingung $b_1 = b_2 \pmod{ggT(r,s)}$ erfüllen, wobei ggT(r,s) den größten gemeinsamen Teiler von r und s bezeichnet,

c) mit Hilfe dir beiden Zahlen b_1 und b_2 nach dem Chinesischen Restwertsatz Werte x_1 und x_2 berechnet werden, die die folgenden Bedingungen erfüllen:

$$x_1 = x \pmod{p} , \quad x_1 = b_1 \pmod{r}$$

$$x_2 = x \pmod{q} , \quad x_2 = b_2 \pmod{s}$$

und anschließend folgende Rechenschritte durchgeführt werden:

$$d\_1 = d \pmod{\phi(p)}$$

$$d\_2 = d \pmod{\phi(q)}$$

$$z_1 = x_1^{d\_1} \pmod{p \cdot r}$$

$$z_2 = x_2^{d\_2} \pmod{q \cdot s}$$

IPR2022-00412
Apple EX1053 Page 692

und $\phi(.)$ die Euler'sche Funktion und kgV(r,s) das kleinste gemeinsame Vielfache von r und s darstellt,

d) anschließend nach dem Chinesischen Restwertsatz aus z_1 und z_2 eine Zahl z berechnet wird mit $z = z_1 \pmod{p \cdot r}$; $z = z_2 \pmod{q \cdot s}$;

e) das Ergebnis E der Exponentiation durch Reduktion von z modulo $p \cdot q$ berechnet wird

f) die vorher berechnete Zahl z (und damit automatisch auch das Ergebnis E) in einem Prüfschritt auf Rechenfehler geprüft wird,

g) der Prüfschritt folgende Rechenoperationen beinhaltet:

g1) Berechnen der Zahlen

$$C_1 = b_1^{d\_1} \pmod{r}$$

$$C_2 = b_2^{d\_2} \pmod{s}$$

wobei d_1 und d_2 vor der Durchführung der modularen Exponentiation modulo $\phi(r)$ bzw. $\phi(s)$ reduziert werden

g2) Vergleich der Werte z_1 und C_1 modulo r sowie z_2 und C_2 modulo s, wobei das Ergebnis der modularen Exponentiation E als fehlerhaft verworfen wird, wenn $C_1 \neq z_1 \bmod r$ oder $C_2 \neq z_2 \bmod s$ gilt.

3. Kryptographisches Verfahren nach Anspruch 2, **dadurch gekennzeichnet,** daß die Zahlen r und s ungerade sind.

4. Kryptographisches Verfahren nach Anspruch 1 bis 3, **dadurch gekennzeichnet,** daß die Zahlen r und s im Bereich $[0, 2^k-1]$ mit $16 \leq k \leq 32$ ausgewählt werden.

5. Kryptographisches Verfahren nach Anspruch 1 bis 4, **dadurch gekennzeichnet,** daß mindestens eine der Zahlen r und s so gewählt wird, daß die

IPR2022-00412
Apple EX1053 Page 693

Binärdarstellung des Produktes p·r beziehungsweise q·s möglichst viele führende Einsen enthält.

6. Kryptographisches Verfahren nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet,** daß beide Zahlen r und s so gewählt werden, daß die Binärdarstellung des Produktes p·r und des Produktes q·s möglichst viele führende Einsen enthalten.

7. Kryptographisches Verfahren nach einem der Ansprüche 5 oder 6, **dadurch gekennzeichnet,** daß

a) in einem ersten Teilschritt zunächst für mindestens eine der Zahlen r und s eine entsprechende optimale Zahl r_{opt} beziehungsweise s_{opt} ohne Beschränkung durch die Bedingung, gemäß der d teilerfremd zu $\phi(kgV(r,s))$ ist, ausgewählt wird, und

b) in einem zweiten Teilschritt jeweils ein benachbarter Wert $r = r_{opt}-i$ beziehungsweise $s = s_{opt}-i$, $i = 0, 1, ..., k$, ausgewählt wird, so daß d teilerfremd zu $\phi(kgV(r,s))$ ist.

8. Kryptographisches Verfahren nach einem der Ansprüche 5 oder 6, **dadurch gekennzeichnet,** daß

a) in einem ersten Teilschritt für jede der Zahlen r und s eine entsprechende optimale Zahl r_{opt} beziehungsweise s_{opt} ohne Beschränkung durch die Bedingung, gemäß der d teilerfremd zu $\phi(kgV(r,s))$ ist, ausgewählt wird, und

b) in einem zweiten Teilschritt jeweils ein Wert $r = 2^l \cdot r_{opt}$ beziehungsweise $s = 2^l \cdot s_{opt}$, $l = 0, 1, ..., j$, ausgewählt wird, so daß d teilerfremd zu $\phi(kgV(r,s))$ ist.

IPR2022-00412
Apple EX1053 Page 694

9. Kryptographisches Verfahren nach einem der Ansprüche 5 oder 6, **dadurch gekennzeichnet,** daß

a) in einem ersten Teilschritt mindestens eine der Zahlen r_{opt} und s_{opt} zunächst ohne Beschränkung durch die Bedingung, gemäß der d teilerfremd zu $\phi(kgV(r,s))$ ist, ausgewählt wird,

b) in einem zweiten Teilschritt jeweils ein benachbarter Wert $r = r_{opt}-i$ beziehungsweise $s = s_{opt}-i$, $i = 0, 1, ..., k$, ausgewählt wird, so daß d teilerfremd zu $\phi(kgV(r,s))$ ist, falls ein solcher Wert für $i = 0, 1,..., k$ existiert, und

c) in einem dritten Teilschritt jeweils ein Wert $r = 2^l \cdot r_{opt}$ beziehungsweise $s = 2^l \cdot s_{opt}$, $i = 0, 1, ..., j$, ausgewählt wird, so daß d teilerfremd zu $\phi(kgV(r,s))$ ist, falls im zweiten Teilschritt kein Wert ausgewählt worden ist.

10. Kryptographisches Verfahren nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet,** daß es das RSA-Verfahren beinhaltet.

11. Kryptographisches Verfahren nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet,** daß es das Rabin'sche-Signaturen-Verfahren beinhaltet.

12. Kryptographisches Verfahren nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet,** daß es das Fiat-Shamir'sche Identifikationsschema-Verfahren beinhaltet.

13. Kryptographische Vorrichtung,

a) mit mindestens einer Exponentiationseinrichtung, die einen eine modulare Exponentiation E

$E = x^d \pmod{p \cdot q}$

enthaltenden Rechenschritt mit einem ersten Primfaktor p, einem zweiten Primfaktor q, einem Exponenten d und einer Basis x ausführt, wobei

b) zur Durchführung der modularen Exponentiation zwei natürliche Zahlen r und s gewählt werden mit der Bedingung , daß d teilerfremd ist zu $\phi(kgV(r,s))$ und wobei die folgenden Rechenschritte durchgeführt werden:

$$x_1 = x \pmod{p \cdot r}$$

$$x_2 = x \pmod{q \cdot s}$$

$$d\_1 = d \pmod{\phi(p \cdot r)}$$

$$d\_2 = d \pmod{\phi(q \cdot s)}$$

$$z_1 = x_1^{d\_1} \pmod{p \cdot r}$$

$$z_2 = x_2^{d\_2} \pmod{q \cdot s},$$

und $\phi(.)$ die Euler'sche Funktion und kgV(r,s) das kleinste gemeinsame Vielfache von r und s darstellt,

c) anschließend nach dem Chinesischen Restwertsatz aus z_1 und z_2 eine Zahl z berechnet wird mit $z = z_1 \pmod{p \cdot r}$; $z = z_2 \pmod{q \cdot s}$;

d) das Ergebnis E der Exponentiation durch Reduktion von z modulo $p \cdot q$ berechnet wird

e) die vorher berechnete Zahl z (und damit automatisch auch das Ergebnis E) in einem Prüfschritt auf Rechenfehler geprüft wird,

f) der Prüfschritt folgende Rechenoperationen beinhaltet:

f1) Berechnen der kleinstmöglichen natürlichen Zahl e mit der Eigenschaft $e \cdot d = 1 \pmod{\phi(kgV(r,s))}$ mit Hilfe des erweiterten Euklid'schen Algorithmus

f2) Berechnen des Wertes $C = z^e \pmod{kgV(r,s)}$

f3) Vergleich der Werte x und C modulo kgV(r,s), wobei das Ergebnis der modularen Exponentiation E als fehlerhaft verworfen wird, wenn $x \neq C \pmod{kgV(r,s)}$.

14. . Kryptographische Vorrichtung,

a) mit mindestens einer Exponentiationseinrichtung, die einen eine modulare Exponentiation E

$E = x^d \pmod{p \cdot q}$

enthaltenden Rechenschritt mit einem ersten Primfaktor p, einem zweiten Primfaktor q, einem Exponenten d und einer Basis x ausführt, wobei

b) zur Durchführung der modularen Exponentiation zwei natürliche Zahlen r und s , sowie zwei Zahlen b_1 und b_2 im Intervall [1,...,r-1] bzw. [1,...,s-1] und teilerfremd zu r bzw. s gewählt werden, und wobei b_1 und b_2 die Bedingung $b_1 = b_2 \pmod{ggT(r,s)}$ erfüllen, wobei ggT(r,s) den größten gemeinsamen Teiler von r und s bezeichnet,

c) mit Hilfe dir beiden Zahlen b_1 und b_2 nach dem Chinesischen Restwertsatz Werte x_1 und x_2 berechnet werden, die die folgenden Bedingungen erfüllen:

$$x_1 = x \pmod{p}, \quad x_1 = b_1 \pmod{r}$$

$$x_2 = x \pmod{q}, \quad x_2 = b_2 \pmod{s}$$

und anschließend folgende Rechenschritte durchgeführt werden:

$$d\_1 = d \pmod{\phi(p)}$$

$$d\_2 = d \pmod{\phi(q)}$$

$$z_1 = x_1^{d\_1} \pmod{p \cdot r}$$

$$z_2 = x_2^{d\_2} \pmod{q \cdot s}$$

und wobei $\phi(.)$ die Euler'sche Funktion und kgV(r,s) das kleinste gemeinsame Vielfache von r und s darstellt,

IPR2022-00412
Apple EX1053 Page 697

d) anschließend nach dem Chinesischen Restwertsatz aus z_1 und z_2 eine Zahl z berechnet wird mit $z = z_1 \pmod{p \cdot r}$; $z = z_2 \pmod{q \cdot s}$;

e) das Ergebnis E der Exponentiation durch Reduktion von z modulo $p \cdot q$ berechnet wird

f) die vorher berechnete Zahl z (und damit automatisch auch das Ergebnis E) in einem Prüfschritt auf Rechenfehler geprüft wird,

g) der Prüfschritt folgende Rechenoperationen beinhaltet:

g1) Berechnen der Zahlen

$$C_1 = b_1^{d\_1} \pmod{r}$$

$$C_2 = b_2^{d\_2} \pmod{s}$$

wobei d_1 und d_2 vor der Durchführung der modularen Exponentiation modulo $\phi(r)$ bzw. $\phi(s)$ reduziert werden,

g2) Vergleich der Werte z_1 und C_1 modulo r sowie z_2 und C_2 modulo s, wobei das Ergebnis der modularen Exponentiation E als fehlerhaft verworfen wird, wenn $C_1 \neq z_1 \bmod r$ oder $C_2 \neq z_2 \bmod s$ gilt.

15. Kryptographische Vorrichtung nach Anspruch 14, **dadurch gekennzeichnet,** daß die Zahlen r und s ungerade sind.

16. Kryptographische Vorrichtung nach Anspruch 13 bis 15, **dadurch gekennzeichnet,** daß die Zahlen r und s im Bereich $[0, 2^k-1]$ mit $16 \leq k \leq 32$ ausgewählt werden.

17. Kryptographische Vorrichtung nach Anspruch 13 bis 16, **dadurch gekennzeichnet,** daß mindestens eine der Zahlen r und s so gewählt wird, daß die Binärdarstellung des Produktes $p \cdot r$ beziehungsweise $q \cdot s$ möglichst viele führende Einsen enthält.

IPR2022-00412
Apple EX1053 Page 698

18. Kryptographische Vorrichtung nach einem der Ansprüche 13 bis 17, **dadurch gekennzeichnet,** daß beide Zahlen r und s so gewählt werden, daß die Binärdarstellung des Produktes p·r und des Produktes q·s möglichst viele führende Einsen enthalten.

19. Kryptographische Vorrichtung nach einem der Ansprüche 17 oder 18, **dadurch gekennzeichnet,** daß

a) in einem ersten Teilschritt zunächst für mindestens eine der Zahlen r und s eine entsprechende optimale Zahl r_{opt} beziehungsweise s_{opt} ohne Beschränkung durch die Bedingung, gemäß der d teilerfremd zu $\phi(kgV(r,s))$ ist, ausgewählt wird, und

b) in einem zweiten Teilschritt jeweils ein benachbarter Wert $r = r_{opt}-i$ beziehungsweise $s = s_{opt}-i$, $i = 0, 1, ..., k$, ausgewählt wird, so daß d teilerfremd zu $\phi(kgV(r,s))$ ist.

20. Kryptographische Vorrichtung nach einem der Ansprüche 17 oder 18, **dadurch gekennzeichnet,** daß

a) in einem ersten Teilschritt für jede der Zahlen r und s eine entsprechende optimale Zahl r_{opt} beziehungsweise s_{opt} ohne Beschränkung durch die Bedingung, gemäß der d teilerfremd zu $\phi(kgV(r,s))$ ist, ausgewählt wird, und

b) in einem zweiten Teilschritt jeweils ein Wert $r = 2^l \cdot r_{opt}$ beziehungsweise $s = 2^l \cdot s_{opt}$, $l = 0, 1, ..., j$, ausgewählt wird, so daß d teilerfremd zu $\phi(kgV(r,s))$ ist.

21. Kryptographische Vorrichtung nach einem der Ansprüche 17 oder 18, **dadurch gekennzeichnet,** daß

IPR2022-00412
Apple EX1053 Page 699

a) in einem ersten Teilschritt mindestens eine der Zahlen r_{opt} und s_{opt} zunächst ohne Beschränkung durch die Bedingung, gemäß der d teilerfremd zu $\phi(kgV(r,s))$ ist, ausgewählt wird,

b) in einem zweiten Teilschritt jeweils ein benachbarter Wert $r = r_{opt}-i$ beziehungsweise $s = s_{opt}-i$, $i = 0, 1, ..., k$, ausgewählt wird, so daß d teilerfremd zu $\phi(kgV(r,s))$ ist, falls ein solcher Wert für $i = 0, 1,..., k$ existiert, und

c) in einem dritten Teilschritt jeweils ein Wert $r = 2^l \cdot r_{opt}$ beziehungsweise $s = 2^l \cdot s_{opt}$, $i = 0, 1, ..., j$, ausgewählt wird, so daß d teilerfremd zu $\phi(kgV(r,s))$ ist, falls im zweiten Teilschritt kein Wert ausgewählt worden ist.

22. Kryptographische Vorrichtung nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet,** daß es das RSA-Verfahren beinhaltet.

23. Kryptographische Vorrichtung nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet,** daß es das Rabin'sche-Signaturen-Verfahren beinhaltet.

24. Kryptographische Vorrichtung nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet,** daß es das Fiat-Shamir'sche Identifikationsschema-Verfahren beinhaltet.

IPR2022-00412
Apple EX1053 Page 700

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 December 2001 (20.12.2001)

PCT

(10) International Publication Number
WO 01/96990 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/EP01/06816

(22) International Filing Date: 15 June 2001 (15.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/594,456 15 June 2000 (15.06.2000) US

(71) Applicant: **RAINBOW TECHNOLOGIES, B.V.** [NL/NL]; Oliphanteweg 10, NL-1397 Le Rotterdam (NL).

(72) Inventors: **ABBOTT, Shawn, D.**; 305 Pinnacle Ridge Place, RR12, Calgary, Alberta T3E 6W3 (CA). **ANDERSON, Allan, D.**; 11158 Bertha Place, Cerritos, CA 90703 (US). **GODDING, Patrick, N.**; 22665 Shady Grove Circle, Lake Forest, CA 92630 (US). **PUNT, Maarten, G.**; 24942 Paseo Arboleda, Lake Forest, CA 92630 (US). **SOTOODEH, Mehdi**; 17 Paloma Drive, Mission Viejo, CA 92692 (US).

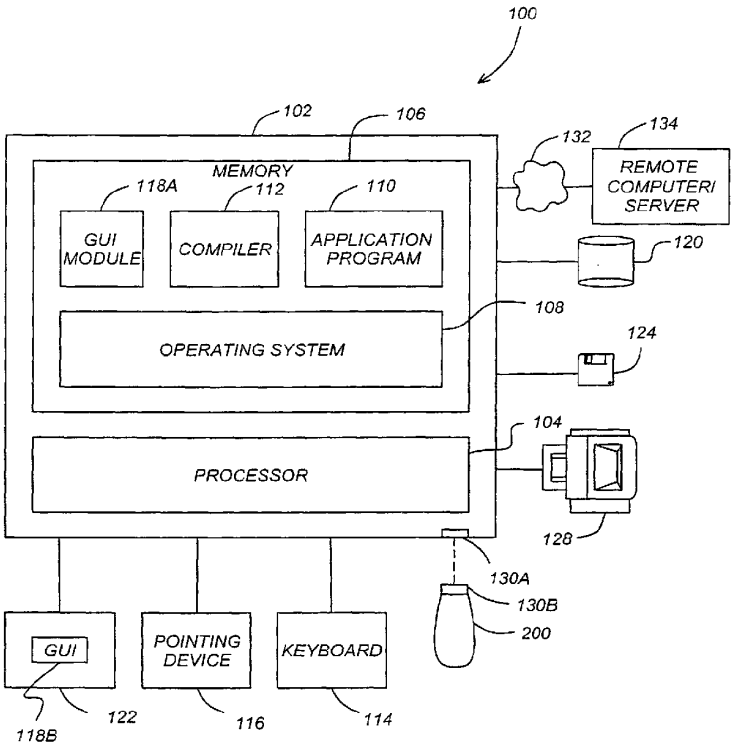
(74) Agents: **SMITH, Samuel, Leonard** et al.; J.A. Kemp & Co., 14 South Square, Gray's Inn, London WC1R 5JJ (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European

[Continued on next page]

(54) Title: USB-COMPLIANT PERSONAL KEY USING A SMARTCARD PROCESSOR AND A SMARTCARD READER EMULATOR



(57) Abstract: A compact, self-contained, personal key is disclosed. The personal key comprises a USB-compliant interface releaseably coupleable to a host processing device operating under command of an operating system; a smartcard processor having a smartcard processor-compliant interface of communicating according to a smartcard input and output protocol; and an interface processor, communicatively coupled to the USB-compliant interface and to the smartcard processor-compliant interface, the interface processor implementing a translation module for interpreting USB-compliant messages into smartcard processor-compliant messages and for interpreting smartcard processor-compliant messages into USB-compliant messages.

WO 01/96990 A2

IPR2022-00412
Apple EX1053 Page 701

patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

USB-COMPLIANT PERSONAL KEY USING A SMARTCARD PROCESSOR AND A SMARTCARD READER EMULATOR

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation-in-part of U.S. Patent Application No. 09/449,159, filed November 24, 1999, by Shawn D. Abbott, Bahram Afghani, Mehdi Sotoodeh, Norman L. Denton III, and Calvin W. Long, and entitled "USB-Compliant Personal Key with Integral Input and Output Devices," which is a continuation-in-part of U.S. Patent Application No. 09/281,017, filed March 30, 1999 by Shawn D. Abbott, Bahram Afghani, Allan D. Anderson, Patrick N. Godding, Maarten G. Punt, and Mehdi Sotoodeh, and entitled "USB-Compliant Personal Key," which claims benefit of U.S. Provisional Patent Application No. 60/116,006, filed January 15, 1999 by Shawn D. Abbott, Barham Afghani, Allan D. Anderson, Patrick N. Godding, Maarten G. Punt, and Mehdi Sotoodeh, and entitled "USB-Compliant Personal Key," all of which applications are hereby incorporated by reference herein.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to computer peripherals, and in particular to an inexpensive USB-compliant personal key that is compatible with existing smartcard processors, drivers, and instruction sets.

2. Description of the Related Art

In the last decade, the use of personal computers in both the home and in the office have become widespread. These computers provide a high level of functionality to many people at a moderate price, substantially surpassing the performance of the large mainframe computers of only a few decades ago. The trend is further evidenced by the increasing popularity of laptop and notebook computers, which provide high-performance computing power on a mobile basis.

IPR2022-00412
Apple EX1053 Page 703

The widespread availability of personal computers has had a profound impact on interpersonal communications as well. Only a decade ago, telephones or fax machines offered virtually the only media for rapid business communications. Today, a growing number of businesses and individuals communicate via electronic mail (e-mail). Personal computers have also been instrumental in the emergence of the Internet and its growing use as a medium of commerce.

While certainly beneficial, the growing use of computers in personal communications, commerce, and business has also given rise to a number of unique challenges. These challenges include the prevention of unauthorized use of software, ensuring the security of e-mail and other electronic communications, as well as Internet commerce.

Smartcards represent a longstanding attempt to deal with at least some of the foregoing challenges. Substantial resources have been made in the design and development of smartcards, smartcard readers, and the associated reader/smartcard drivers which allow computer applications to interface with the smartcard to perform security and data storage functions. Even so, smartcards have not enjoyed widespread popularity. Smartcard readers are relatively expensive, and not widely available. Further, the lack of uniform smartcard/smartcard reader physical interface standards have resulted in smartcard/smartcard reader physical interface compatibility problems, many of which remain unresolved.

USB-compliant personal keys, such as that which is disclosed in co-pending and commonly assigned U.S. Patent Application Nos. 09/449,159 and 09/281,017, described above, offer the benefit of smartcard functionality in a universally accepted USB form factor. The Universal Serial Bus (USB) is a connectivity standard developed by computer and telecommunication industry members for interfacing computers and peripherals. USB-compliant devices allow the user to install and hot-swap devices without long installation procedures and reboots, and features a 127 device bus capacity, dual-speed data transfer, and can provide limited power to devices attached on the bus. Because the USB connectivity standard is rapidly

IPR2022-00412
Apple EX1053 Page 704

becoming available on most personal computers, it offers a standard, widely available physical interface, the unavailability of which has prevented smartcards from achieving widespread acceptance.

While smartcards have not enjoyed widespread popularity in the United States, they are widely accepted in Europe. Hence, many software applications and drivers have been developed for existing smartcard-based devices and their readers. Unfortunately, smartcard interface protocols such as those described in ISO 7816 are incompatible with the USB protocols used in the above-described devices. This incompatibility has led to two unfortunate consequences. First, to comply with USB interface protocol requirements, current USB-compliant personal keys utilize special purpose processors, instead of the low cost, limited capability processors currently available for smartcards. This increases the cost of the USB-compliant personal key, making widespread acceptance more difficult. Also, because each USB-compatible personal key may use a different processor (and different instruction sets), users may require different device drivers for different personal keys. This too represents another barrier to widespread acceptance of the personal key.

From the foregoing, it is apparent that there is a need for a USB-compliant personal key that is usable with legacy personal identification devices, such as processors having smartcard processors and/or those complying with the ISO 7816. There is also a need for a USB-compliant personal key that makes maximum use of existing smartcard protocols, software and devices wherever possible, and which retain at least a limited compatibility with existing devices designed to interface with smartcards. The present invention satisfies that need.

SUMMARY OF THE INVENTION

The present invention satisfies all of these needs with a personal key in a form factor that is compliant with a commonly available I/O interface such as the Universal Serial Bus (USB) and at the same time, usable with existing smartcard software applications. The personal key comprises a USB-compliant interface releaseably

IPR2022-00412
Apple EX1053 Page 705

coupleable to a host processing device operating under command of an operating system; a smartcard processor having a smartcard processor-compliant interface for communicating according to a smartcard input and output protocol; and an interface processor, communicatively coupled to the USB-compliant interface and to the smartcard processor-compliant interface, the interface processor implementing a translation module for interpreting USB-compliant messages into smartcard processor-compliant messages and for interpreting smartcard processor-compliant messages into USB-compliant messages.

In one embodiment, the method comprises the steps of accepting a message comprising a smartcard reader command selected from a smartcard reader command set from a host computer operating system in a virtual smartcard reader; packaging the message for transmission via a USB-compliant interface according to a first message transfer protocol; transmitting the packaged message to a personal key communicatively coupled to the USB-compliant interface; receiving the packaged message in the personal key; unpackaging the message in the personal key to recover the smartcard reader command; translating the smartcard reader command into a smartcard command within the personal key; and providing the smartcard command to the smartcard processor.

The present invention is well suited for controlling access to network services, or anywhere a password, cookie, digital certificate, or smartcard might otherwise be used, including:

- Remote access servers, including Internet protocol security (IPSec), point to point tunneling protocol (PPTP), password authentication protocol (PAP), challenge handshake authentication protocol (CHAP), remote access dial-in user service (RADIUS), terminal access controller access control system (TACACS);
- Providing Extranet and subscription-based web access control, including hypertext transport protocol (HTTP), secure sockets layer (SSL);

IPR2022-00412
Apple EX1053 Page 706

- Supporting secure online banking, benefits administration, account management;
- Supporting secure workflow and supply chain integration (form signing);
- Preventing laptop computer theft (requiring personal key for laptop operation);
- Workstation logon authorization;
- Preventing the modification or copying of software;
- Encrypting files;
- Supporting secure e-mail, for example, with secure multipurpose Internet mail extensions (S/MIME), and open pretty good privacy (OpenPGP)
- Administering network equipment administration; and
- Electronic wallets, with, for example, secure electronic transaction (SET, MilliCent, eWallet)

BRIEF DESCRIPTION OF THE DRAWINGS

Referring now to the drawings in which like reference numbers represent corresponding parts throughout:

FIG. 1 is a diagram showing an exemplary hardware environment for practicing the present invention;

FIG. 2 is a block diagram of a personal key communicatively coupled to a host computer;

FIG. 3 is a block diagram of a personal key with a smartcard processor communicatively coupled to a host computer; and

FIGs. 4A-4D are flow charts presenting exemplary method steps that can be used to practice the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

In the following description, reference is made to the accompanying drawings which form a part hereof, and which is shown, by way of illustration, several

IPR2022-00412
Apple EX1053 Page 707

embodiments of the present invention. It is understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present invention.

FIG. 1 illustrates an exemplary computer system 100 that could be used to implement the present invention. The host computer 102 comprises a processor 104 and a memory, such as random access memory (RAM) 106. The host computer 102 is operatively coupled to a display 122, which presents images such as windows to the user on a graphical user interface 118B. The host computer 102 may be coupled to other devices, such as a keyboard 114, a mouse device 116, a printer 128, etc. Of course, those skilled in the art will recognize that any combination of the above components, or any number of different components, peripherals, and other devices, may be used with the host computer 102.

Generally, the host computer 102 operates under control of an operating system 108 stored in the memory 106, and interfaces with the user to accept inputs and commands and to present results through a graphical user interface (GUI) module 118A. Although the GUI module 118A is depicted as a separate module, the instructions performing the GUI functions can be resident or distributed in the operating system 108, the computer program 110, or implemented with special purpose memory and processors. The host computer 102 also implements a compiler 112 which allows an application program 110 written in a programming language such as COBOL, C++, FORTRAN, or other language to be translated into processor 104 readable code. After completion, the application 110 accesses and manipulates data stored in the memory 106 of the host computer 102 using the relationships and logic that are generated using the compiler 112. The host computer 102 also comprises an input/output (I/O) port for a personal token 200 (hereinafter alternatively referred to also as a personal key 200). In one embodiment, the I/O port is a USB-compliant interface comprising a host computer USB-compliant interface 130A and a personal token USB-compliant interface 130B (hereinafter referred to collectively as the USB-compliant interface 130.

IPR2022-00412
Apple EX1053 Page 708

In one embodiment, instructions implementing the operating system 108, the computer program 110, and the compiler 112 are tangibly embodied in a computer-readable medium, e.g., data storage device 120, which could include one or more fixed or removable data storage devices, such as a zip drive, floppy disc drive 124, hard drive, CD-ROM drive, tape drive, etc. Further, the operating system 108 and the computer program 110 are comprised of instructions which, when read and executed by the computer 102, causes the computer 102 to perform the steps necessary to implement and/or use the present invention. Computer program 110 and/or operating instructions may also be tangibly embodied in memory 106 and/or data communications devices, thereby making a computer program product or article of manufacture according to the invention. As such, the terms "article of manufacture" and "computer program product" as used herein are intended to encompass a computer program accessible from any computer readable device or media.

The host computer 102 may be communicatively coupled to a remote computer or server 134 via communication medium 132 such as a dial-up network, a wide area network (WAN), local area network (LAN), virtual private network (VPN) or the Internet. Program instructions for computer operation, including additional or alternative application programs can be loaded from the remote computer/server 134. In one embodiment, the computer 102 implements an Internet browser, allowing the user to access the world wide web (WWW) and other internet resources.

Those skilled in the art will recognize that many modifications may be made to this configuration without departing from the scope of the present invention. For example, those skilled in the art will recognize that any combination of the above components, or any number of different components, peripherals, and other devices, may be used with the present invention.

FIG. 2 is a block diagram illustrating the components of one embodiment of a personal key 200. The personal key 200 communicates with and obtains power from the host computer 102 through a USB-compliant communication path in the USB-compliant interface 130 which includes the input/output port 130A of the host

IPR2022-00412
Apple EX1053 Page 709

computer 102 and a matching input/output (I/O) port 130B on the personal key 200. The processor 212 is communicatively coupled to a memory 214, which stores data and instructions to implement the above-described features of the invention. In one embodiment, the memory 214 is a non-volatile random-access memory that can retain factory-supplied data as well as customer-supplied application related data. The processor 212 may also include some internal memory for performing some of these functions.

The processor 212 is optionally communicatively coupled to an input device 218 via an input device communication path 224 and to an output device 222 via an output device communication path 224, both of which are distinct from the USB-compliant interface 130. These separate communication paths 220 and 224 allow the user to view information about processor 212 operations and provide input related to processor 212 operations without allowing a process or other entity with visibility to the USB-compliant interface 130 to eavesdrop or intercede. This permits secure communications between the key processor 212 and the user. In one embodiment of the invention set forth more fully below, the user communicates directly with the processor 212 by physical manipulation of mechanical switches or devices actuatable from the external side of the key (for example, by pressure-sensitive devices such as buttons and mechanical switches). In another embodiment of the invention set forth more fully below, the input device includes a wheel with tactile detents indicating the selection of characters.

The input device and output devices 218, 222 may cooperatively interact with one another to enhance the functionality of the personal key 200. For example, the output device 222 may provide information prompting the user to enter information into the input device 218. For example, the output device 222 may comprise a visual display such as an alphanumeric LED or LCD display (which can display Arabic numbers and or letters) and/or an aural device. The user may be prompted to enter information by a beeping of the aural device, by a flashing pattern of the LED, or by both. The output device 222 may also optionally be used to confirm entry of

IPR2022-00412
Apple EX1053 Page 710

information by the input device 218. For example, an aural output device may beep when the user enters information into the input device 218 or when the user input is invalid. The input device 218 may take one of many forms, including different combinations of input devices.

Although the input device communication path 220 and the output device communication path 224 are illustrated in FIG. 2 as separate paths, the present invention can be implemented by combining the paths 220 and 224 while still retaining a communication path distinct from the USB-compliant interface 130. For example, the input device 218 and output device 222 may be packaged in a single device and communications with the processor 212 multiplexed over a single communication path.

FIG. 3 is a block diagram of the personal key 200 and host computer 102 as applied to the present invention. Unlike the personal key 200 illustrated in FIG. 2, the personal key 300 illustrated in FIG. 3 comprises a smartcard processor 320. The smartcard processor 300 is a processor which complies with well-known smartcard I/O protocols and smartcard command sets and functions, such as those described by the International Standards Organization (ISO) standard 7816 Part III (defining electronic properties and transmission characteristics), which is hereby incorporated by reference herein.

Physically, the smartcard compliant I/O interface 324 includes a serial I/O line, a reset (RST) line, a clock (CLK) line, a programming voltage (VPP), a power supply voltage (VCC) and a ground. This I/O interface 324 is further described in the publication "Introduction to Smartcards" by Dr. David B. Everett, which was published in 1999 by the Smart Card News Ltd., and is incorporated by reference herein.

As was the case with the personal key 200 and host computer 102 illustrated in FIG. 1, the present invention allows the use of a personal key 300 communicating with the host computer 102 via a USB-compliant interface 130. However, the substitution of the smartcard processor 320 for the ordinary processor 212 depicted in

IPR2022-00412
Apple EX1053 Page 711

FIG. 2 has several advantages. First, smartcard processors 212 are relatively inexpensive and readily available. Second, a large number of application programs 110 have been developed for the use of smartcards, including the personal computer/smartcard (PC/SC) interface developed by the MICROSOFT CORPORATION. By providing a smartcard processor (which complies with the smartcard I/O protocols and supports smartcard command sets), this software can be used with a personal key 300 in a USB-compliant form factor.

The use of the smartcard processor 320 in the personal key 300 is enabled by use of an interface processor 314 communicatively coupled to the smartcard processor 320 via a smartcard-compatible (S/C 7816) interface 324. The interface processor 314 comprises a smartcard reader emulator module (SREM) 316 and a translation module 318. The SREM 316 implements functions that emulate those of a smartcard reader, thus projecting the image of a smartcard reader to the smartcard processor 320. The SREM 316 provides all instructions and commands to the smartcard processor 320 and receives messages and responses from the smartcard processor 320 according to the S/C protocol.

The host computer 102 comprises a virtual smartcard reader module (VSRM) 302. The VSRM comprises a communication module 312, an answer-to-reset module 308, and a smartcard insertion/removal reporting module 306. The communication module 312 packages messages intended for the personal key 300 for transmission via the USB-compliant interface. In one embodiment, messages and commands that are sent to the personal key 300 packaged as:

USB command = USB header + USB cdata (wherein USB cdata is the smartcard compliant command)

IPR2022-00412
Apple EX1053 Page 712

and messages and responses from the personal key 300 are packaged as:

USB response = USB header + USB rdata (wherein USB rdata is the smartcard compliant response)

These packaged messages are unpacked by the translation module 318 in the personal key 300. Similarly, messages transmitted by the smartcard processor 320 to the host computer 102 are packaged by the translation module 318 and unpackaged by the communication module 312 before being provided to the operating system 108, the application program interface 260, and the application 110 using the personal key 300 to perform operations.

Just as the SREM 316 emulates the presence of a smartcard reader for the smartcard processor 320, the VSRM 302 emulates the presence of a smartcard reader to the OS 108 in the host computer 102. These functions are accomplished in the bootup module 311, the insert/remove module 306, the answer-to-reset module 308, and the PTS module 310.

As a part of a normal bootup sequence, the host computer's 102 operating system performs a startup sequence to determine which hardware elements are available for use. In prior art smartcard systems, the smartcard reader remains coupled to the host computer 102, whether a smartcard is inserted into the reader or not. Hence, the smartcard reader can respond to startup sequence queries, and the smartcard reader is recognized by the operating system 108 for further operations. However, in the present invention, there is no smartcard reader to answer to the bootup query, and the operating system would ordinarily be unable to operate with a smartcard thereafter. To solve this problem, the present invention comprises a bootup module 311, which responds to messages from the operating system 108 in the same way as a smartcard reader would if it were coupled to the host computer 102.

Similarly, the insert/remove module 306 provides an indication to the operating system 108 that the personal key 300 has been inserted or removed from the

IPR2022-00412
Apple EX1053 Page 713

USB-compliant interface 130. This is accomplished by querying the host computer USB-compliant interface port 130A.

When a software application calls 110, via API 260 and the operating system 108 invokes a command that calls for a smartcard related function, the smartcard reader passes a reset command to the smartcard. The smartcard returns an answer-to-reset message which indicates, among other things, the protocol and I/O interface supported by the attached smartcard.

The reset signal is used to start up the program contained in a memory 322 communicatively coupled to or resident within the smartcard processor 320. The ISO standard defines three reset modes, internal reset, active low reset, and synchronous high active reset. Most smartcard processors 320 operate using the active low reset mode. In this mode, the smartcard processor 320 transfers control to the entry address for the program when the reset signal returns to the high voltage level. The synchronous mode of operation is more commonly met with smartcards used for telephonic applications.

The sequence of operations for activating the smartcard processor 320 is defined in order to minimize the possibility of damaging the smartcard processor 320. Of particular importance is avoiding corruption of the non-volatile memory 322 of the smartcard. Most smartcard processors 320 operate using an active low reset mode in which the smartcard processor 320 transfers control to the entry address for the program when the reset signal returns to the high voltage level. The sequence performed by the smartcard processor includes the steps of setting the RST line low, applying VCC to the proper supply voltage, setting the I/O in the receive mode, setting VPP in the idle mode, applying the clock, and taking the RST line high (active low reset).

In prior art smartcard systems, after the reset signal is applied by the smartcard reader, the smartcard processor 320 responds with an answer-to-reset message. For the active low reset mode, the smartcard processor 320 should respond between 400 and 40,000 clock cycles after the rising edge of the reset signal. The answer-to-reset

IPR2022-00412
Apple EX1053 Page 714

signal is at most 33 characters, and includes 5 fields including an initial character (TS), a format character (TO), interface characters (TAi, TBi, TCi, and TDi), historical characters (T1, T2, ... , TK), and a check character (TCK). Among other things, the answer-to-reset signal provides an indication of the smartcard protocol(s) which are supported smartcard processor. Typical smartcard protocols include the T=0 protocol (asynchronous half duplex byte transmission) and T=1 (asynchronous half duplex block transmission).

In the embodiment of the present invention shown in FIG. 3, the reset signal is provided by the VSRM 302, packaged by the communication module 312, and sent via the USB-compliant interface 130B to the personal key 300. The message is unwrapped by the translation module 318. Then, the smartcard reader emulation module activates the RST signal path in the smartcard interface 324, thus providing the RST command to the smartcard processor 320. The smartcard processor 320 responds with an answer-to-reset message, sends the message via the serial I/O line of the smartcard interface 324 to the interface processor 314. The message is then packaged by the translation module 318 and transmitted to the host computer 102 via the USB-compliant interface 326. The message is then unpackaged by the communication module 312 and provided to the operating system 108 and ultimately, the application 110 that requested the use of the smartcard.

In another embodiment of the present invention, the personal key 300 does not comprise a smartcard processor 320, but rather a special purpose processor which does not respond to messages and commands in the smartcard I/O protocol (such as that which is illustrated in FIG. 1). The present invention can still be used with existing smartcard applications 110, however, because the VSRM 302 and the interface processor 314 can be used to simulate the presence of a smartcard processor 320. When the smartcard software application 110 desires use of the personal key 300, the VSRM accepts the reset command from the PC/SC modules in the operating system 108, translates the reset message into a functionally equivalent message for the special purpose processor in the personal key 300, and transmits the message to the

IPR2022-00412
Apple EX1053 Page 715

personal key 300. After the personal key 300 is activated, it sends a message indicating as such to the host computer 102. The VSRM 302, and translates this message to a response that is compatible with the smartcard application 110, namely, an ATR message. Alternatively, the smartcard command to special purpose processor command translation can occur in the emulation processor 314 in the personal key 300.

Returning to the embodiment disclosed in FIG. 3, after the smartcard processor has issued the ATR message, a protocol type selection (PTS) message may be sent to the smartcard processor 320. The PTS message from the OS 108 is received by the PTS module 310 in the VSRM 302, packaged for transmission via the USB-compliant interface 130 to the personal key 300, where it is unpackaged and provided to the smartcard processor 320. The smartcard provides a response consistent with the ISO standards to the emulation module 316. The response is packaged, and transmitted over the USB-compliant interface 130 to the host computer 102, where it is unpackaged by the communication module 312 and provided to the operating system.

FIGs. 4A-4D are flow charts presenting exemplary method steps used to practice one embodiment of the present invention. When the host computer 102 is booted up, the virtual smartcard reader 302 accepts 402 a bootup query from the host computer's operating system 108. Although a smartcard reader is not communicatively coupled to the host computer 130 the virtual smartcard reader 302 emulates the existence of a smartcard reader and provides an indication that a smartcard reader is available to the OS 108. Consequently, when the bootup procedures are completed, a smartcard reader will be registered as an available device to smartcard applications 110.

When the host computer is booted up, a personal key 300 may or may not be communicatively coupled to the USB-compliant interface 130. When a personal key 300 is not attached, the VSRM 302 provides 404 the same indication to the operating system 108 as would be supplied by a smartcard reader without an inserted smartcard. This is accomplished by receiving 406 an indication that the personal key has been

IPR2022-00412
Apple EX1053 Page 716

communicatively coupled to the USB-compliant interface, and providing an indication to the host computer operating system. Since the VSRM is emulating the functions of a smartcard, the indication is provided 408 to the host computer operating system (or equivalently, the personal computer/smartcard (PC/SC) interface modules therein) is that of an insert event.

If desired and the smartcard processor 320 supports multiple protocols, a protocol type selection (PTS) command may be issued by the operating system 108. The VSRM 302 receives 410 the PTS command, packages the command for transmission to the personal key 300 via the USB-compliant interface 130. The wrapped PTS command is then transmitted over the USB-compliant interface 130 and received by the personal key 300. The PTS command is unwrapped by the translate module 318 in the interface processor 314 and provided to the smartcard processor 320 via the smartcard-compliant interface 324. The smartcard processor computes the appropriate response, sends the response to the interface processor 314, where the response is packaged by the translate module 318 for transmission to the host computer 102 via the USB-compliant interface 130. The communication module 312 unpackages the response, and the PTS module 310 formats the response, if necessary, to be consistent with a PTS response received from a smartcard reader. The formatted response is then provided 412 to the OS 108.

FIG. 4B is a flow chart describing exemplary method steps used to provide commands and/or data from the OS 108 to the smartcard processor 320 and from the smartcard processor 320 to the OS 108. A message, which may comprise a smartcard reader command belonging to a smartcard reader command set is accepted 414 from a host computer operating system 108 in the virtual smartcard reader module (VSRM) 302. The message is packaged 416 for transmission via the USB-compliant interface 130 according to a first message transfer protocol.

The packaged message is then transmitted 418 to the communicatively coupled personal key 300 via the USB-compliant interface 130. The packaged message is received 420 and unpackaged 422 in the personal key 300. If the

IPR2022-00412
Apple EX1053 Page 717

smartcard reader command requires additional processing before being forwarded to the smartcard processor 320, the smartcard reader command is translated 424 into a smartcard command within the personal key 300 before being provided 426 to the smartcard processor 320.

The smartcard processor 320 then performs the indicated operation, and a response is accepted 428 from the smartcard processor 320. If the smartcard response requires further processing by a smartcard reader, the smartcard response is translated 430 into a smartcard reader response. The smartcard reader response is then packaged 432 and transmitted 434 to the host computer 102 via the USB-compliant interface 130. The host computer 102 receives 436 and unpackages 438 the message and provides 440 the response to the smartcard software application 110 that issued the command.

Next, when the personal key 300 is removed, the VSRM 302 reports 444 an indication to the OS 108 that the "virtual smartcard" (the personal key 300) has been removed. The provided indication is the same as that which would be provided by a smartcard reader when a smartcard is removed. The indication can be obtained, for example by receiving 442 an indication from a USB driver or other device indicating the removal of a USB device.

In summary, Tables I and II provides an summary of the communication protocol for an OS 108 command from the host computer 102 to the smartcard processor 320 in the personal key (Table I), and for a smartcard processor 320 response to the operating system 108.

IPR2022-00412
Apple EX1053 Page 718

Step	Description
1	Smartcard reader command issued from OS 108 is passed to VSRM 302
2	VSRM 302 adds a USB header, and creates a USB command
3	VSRM's 302 communication module 312 sends the USB command to the personal key 300
4	The translation module 318 strips off the USB header and recovers the smartcard command
5	The smartcard command is sent to the smartcard processor 320
6	The smartcard processor 320 executes the function requested by the smartcard command

Table I

Step	Description
1	Smartcard processor 320 generates a smartcard response
2	The smartcard response is sent from the smartcard processor 320 to the translation module 318
3	The translation module 318 adds a USB header to create a USB response
4	The USB response is transmitted to the VSRM 302
5	The communication module 312 strips off the USB header and recovers the smartcard response
6	The smartcard response is transmitted to the OS 108

Table II

IPR2022-00412
Apple EX1053 Page 719

Tables III and IV provides a summary of the communication protocol for a request from an application program 110 to the smartcard processor 320 and for a request from an application program 110 to the smartcard processor 320.

Step	*Description*
1	Smartcard processor 320 command from the application program 110 is sent to the OS 108 via an API 260
2	The smartcard processor 320 command is sent from the OS 108 to the VSRM 302
3	The VSRM 302 adds a USB header to the smartcard processor 320 command to create a USB-compatible command
4	The VSRM's comm module 312 sends the USB-compliant command to the personal key 300
5	Translation module 318 strips off the USB header and recovers the smartcard processor command
6	The smartcard processor command is transmitted to the smartcard processor 320
7	The smartcard processor 320 performs the function indicated by the smartcard processor command

Table III

IPR2022-00412
Apple EX1053 Page 720

Step	Description
1	The smartcard processor 320 generates a response to the smartcard processor command
2	The response is provided to the translation module 318
3	The translation module adds a USB header to create a USB-compatible smartcard processor response
4	The USB-compatible smartcard processor response is sent to the VSRM 302
5	The communication module 312 strips off the USB header to recover the smartcard processor response
6	The smartcard processor response is provided to the application 110 via the OS 108 and the API 260

Table IV

Conclusion

This concludes the description of the preferred embodiments of the present invention. In summary, the present invention describes a personal key comprising a USB-compliant interface releaseably coupleable to a host processing device operating under command of an operating system; a smartcard processor having a smartcard processor-compliant interface for communicating according to a smartcard input and output protocol; and an interface processor, communicatively coupled to the USB-compliant interface and to the smartcard processor-compliant interface, the interface processor implementing a translation module for interpreting USB-compliant

IPR2022-00412
Apple EX1053 Page 721

messages into smartcard processor-compliant messages and for interpreting smartcard processor-compliant messages into USB-compliant messages. In another embodiment, the invention is described by a method comprising the steps of accepting a message comprising a smartcard reader command selected from a smartcard reader command set from a host computer operating system in a virtual smartcard reader; packaging the message for transmission via a USB-compliant interface according to a first message transfer protocol; transmitting the packaged message to a personal key communicatively coupled to the USB-compliant interface; receiving the packaged message in the personal key; unpackaging the message in the personal key to recover the smartcard reader command; translating the smartcard reader command into a smartcard command within the personal key; and providing the smartcard command to the smartcard processor.

The foregoing description of the preferred embodiment of the invention has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed. Many modifications and variations are possible in light of the above teaching. It is intended that the scope of the invention be limited not by this detailed description, but rather by the claims appended hereto. The above specification, examples and data provide a complete description of the manufacture and use of the composition of the invention. Since many embodiments of the invention can be made without departing from the spirit and scope of the invention, the invention resides in the claims hereinafter appended.

IPR2022-00412
Apple EX1053 Page 722

WHAT IS CLAIMED IS:

1. A compact personal token (300), comprising:

a USB-compliant interface (130B) releaseably coupleable to a host processing device (102) operating under command of an operating system (108);

a smartcard processor (320) having a smartcard processor-compliant interface (324) for communicating according to a smartcard input and output protocol;

an input device (218) communicatively coupled to the smartcard processor for providing secure input to the processor;

an interface processor (314), communicatively coupled to the USB-compliant interface (130B) and to smartcard processor-compliant interface (324) the interface processor (314) implementing a translation module (318) for interpreting USB-compliant messages into smartcard processor-compliant messages and for interpreting smartcard processor-compliant messages into USB-compliant messages.

2. The apparatus of claim 1, wherein the interface processor (314) emulates a smartcard reader to the smartcard processor (320).

3. The apparatus of claim 1, wherein:

the host processing device (102) comprises a virtual smartcard reader in communication with the operating system, the virtual smartcard reader for emulating a smartcard reader communicatively coupled to the host processing device (102) and including a communication module (312) for packaging messages for transmission to the personal token (300) via the USB compliant interface (130) according to a first protocol and for unpackaging messages received from the personal token (300) via the USB-compliant interface according to the first protocol; and

the interface processor translation module (318) unpackages messages from the host processing device (102) according to the first protocol and packages messages destined for the host processing device (102) according to the first protocol.

IPR2022-00412
Apple EX1053 Page 723

4. The apparatus of claim 3, wherein the virtual smartcard reader further comprises a bootup module (311) for responding to an operating system bootup procedure with an indication that a smartcard reader is communicatively coupled to the host processor.

5. The apparatus of claim 3, wherein the virtual smartcard reader further comprises an answer-to-reset (ATR) module (308) for providing an ATR message to the operating system (108) in response to a reset message.

6. The apparatus of claim 3, wherein the virtual smartcard reader further comprises a reporting module for receiving and reporting the insertion of the personal token in a USB-compliant port communicatively coupled to the host processor (102) and the removal of the personal token as a removal of a smartcard from a smartcard reader.

7. The apparatus of claim 3, wherein the virtual smartcard reader further comprises a protocol selection module for receiving a protocol type selection (PTS) command from the operating system and providing a PTS response message to the operating system (108).

8. A method of communicating between a smartcard processor (320) in a personal key (300) communicatively coupled to a host computer (102) via a USB-compliant interface (130), comprising the steps of:

accepting a message comprising a smartcard reader command selected from a smartcard reader command set from a host computer operating system (108) in a virtual smartcard reader;

packaging the message for transmission via a USB-compliant interface (130) according to a first message transfer protocol;

IPR2022-00412
Apple EX1053 Page 724

transmitting the packaged message to a personal key (300) communicatively coupled to the USB-compliant interface (130);

receiving the packaged message in the personal key (300);

unpackaging the message in the personal key (300) to recover the smartcard reader command;

translating the smartcard reader command into a smartcard command within the personal key (300); and

providing the smartcard command to the smartcard processor (320);

accepting a user input to the smartcard processor (320) via an input device (218) communicatively coupled to the smartcard processor (320) via an input communication device communication path distinct from the USB-compliant interface (130);

accepting a smartcard response from the smartcard processor (320);

translating the smartcard response into a smartcard reader response;

packaging the smartcard reader response for transmission to the host processor (102) via the USB-compliant interface (130);

transmitting the packaged message from the personal key (300) to the host processor (102);

receiving the packaged message in the host computer (102);

unpackaging the smartcard reader response; and

providing the smartcard reader response to the host processor operating system (108).

IPR2022-00412
Apple EX1053 Page 725

9. The method of claim 8, further comprising the steps of:

accepting a startup query from the host computer operating system (108) in the virtual smartcard reader; and

providing an indication that a smartcard reader is communicatively coupled to the host computer to the host computer operating system (108).

10. The method of claim 9, further comprising the steps of:

receiving an indication that the personal key (300) has been communicatively coupled to the USB-compliant interface (130);

reporting the indication that the personal key (300) is communicatively coupled to the USB-compliant interface (130) to the host processor operating system (108) as the insertion of a smartcard;

receiving an indication that the personal key (300) has been communicatively decoupled from the USB-compliant interface (130); and

reporting the indication that the personal key has been communicatively decoupled from the USB-compliant interface (130) to the host processor operating system (108) as the removal of the smartcard.

11. The method of claim 8, further comprising the steps of:

receiving a protocol type selection (PTS) command from the host computer operating system (108); and

providing a PTS response message to the operating system (108).

IPR2022-00412
Apple EX1053 Page 726

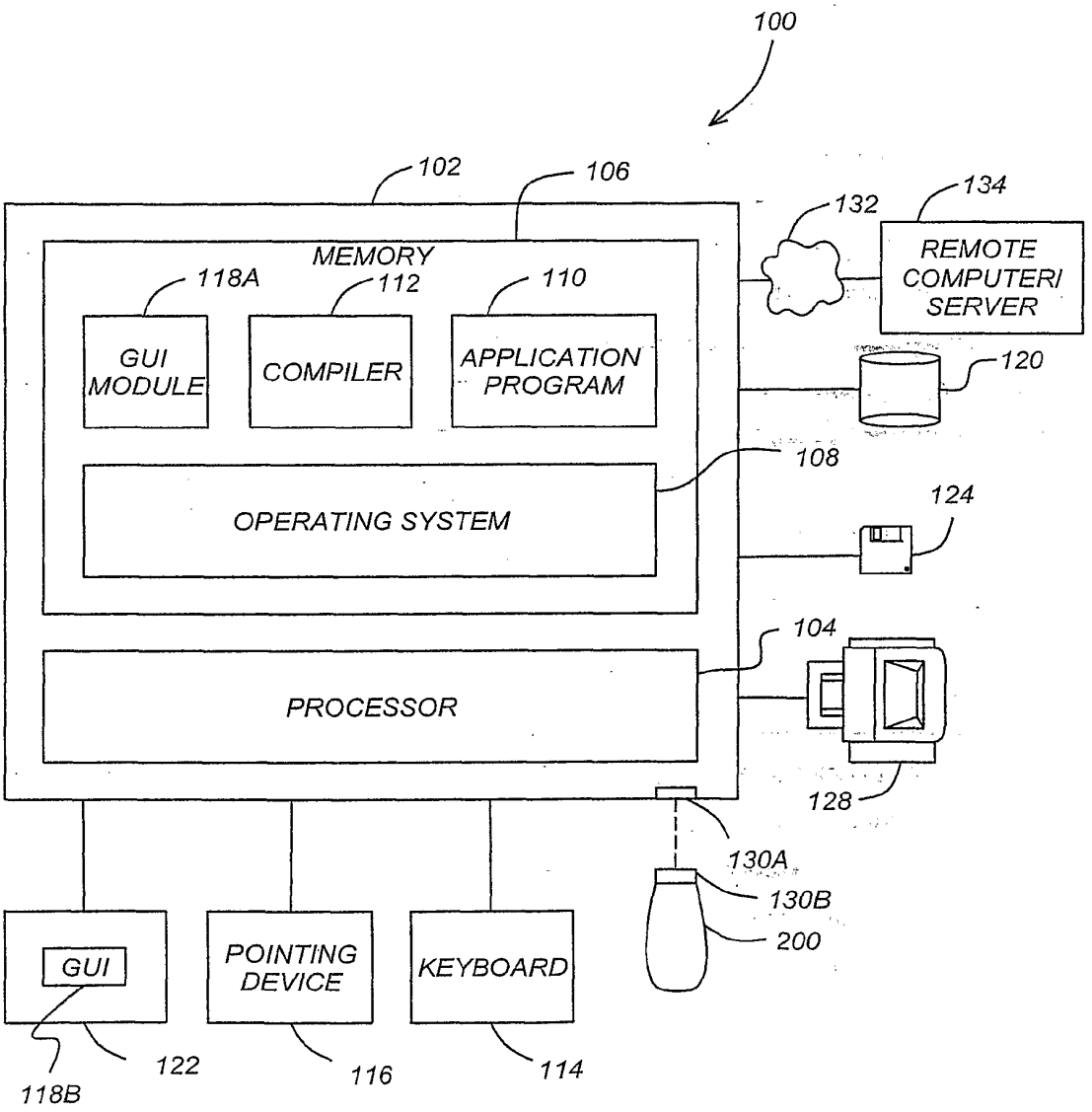

100
102
106
MEMORY
118A
112
110
GUI MODULE
COMPILER
APPLICATION PROGRAM
OPERATING SYSTEM
108
PROCESSOR
104
132
134
REMOTE COMPUTER/ SERVER
120
124
128
130A
130B
200
GUI
POINTING DEVICE
KEYBOARD
118B
122
116
114

FIG. 1

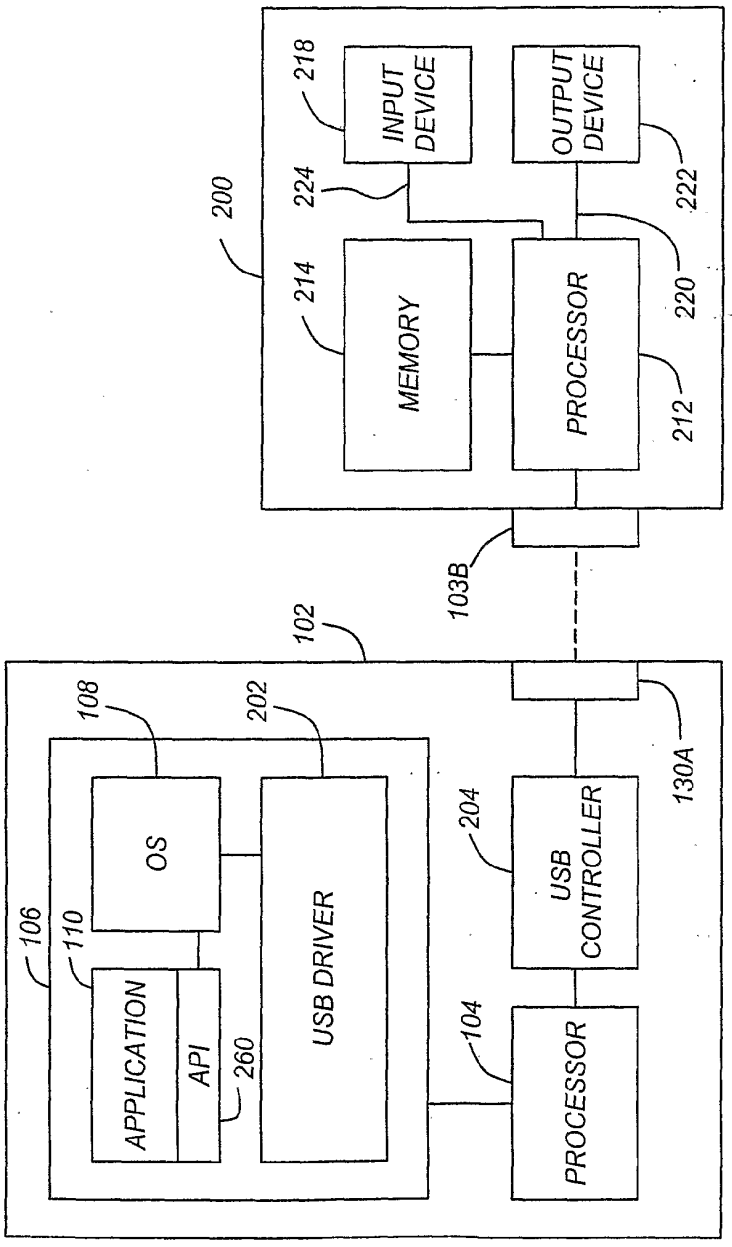
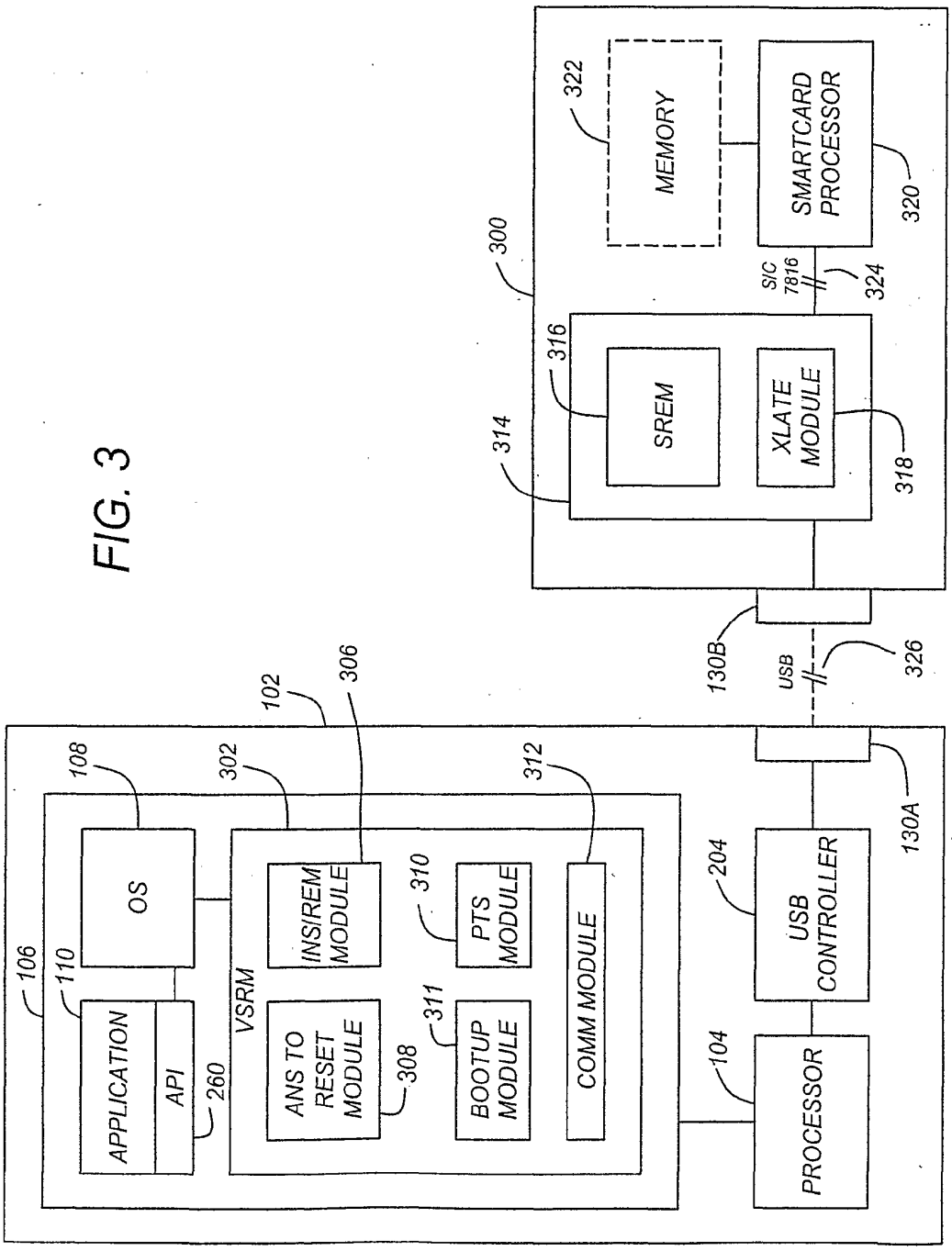

200
218
INPUT DEVICE
OUTPUT DEVICE
224
222
214
MEMORY
PROCESSOR
220
212
103B
102
108
202
OS
USB DRIVER
204
USB CONTROLLER
130A
106
110
APPLICATION
API
260
104
PROCESSOR

FIG. 2

FIG. 3


102
106
108
110
APPLICATION
API
260
OS
302
VSRM
306
INS/REM MODULE
308
ANS TO RESET MODULE
310
PTS MODULE
311
BOOTUP MODULE
312
COMM MODULE
104
PROCESSOR
204
USB CONTROLLER
130A
USB
326
130B
300
314
316
SREM
XLATE MODULE
318
S/C 7816
324
322
MEMORY
SMARTCARD PROCESSOR
320

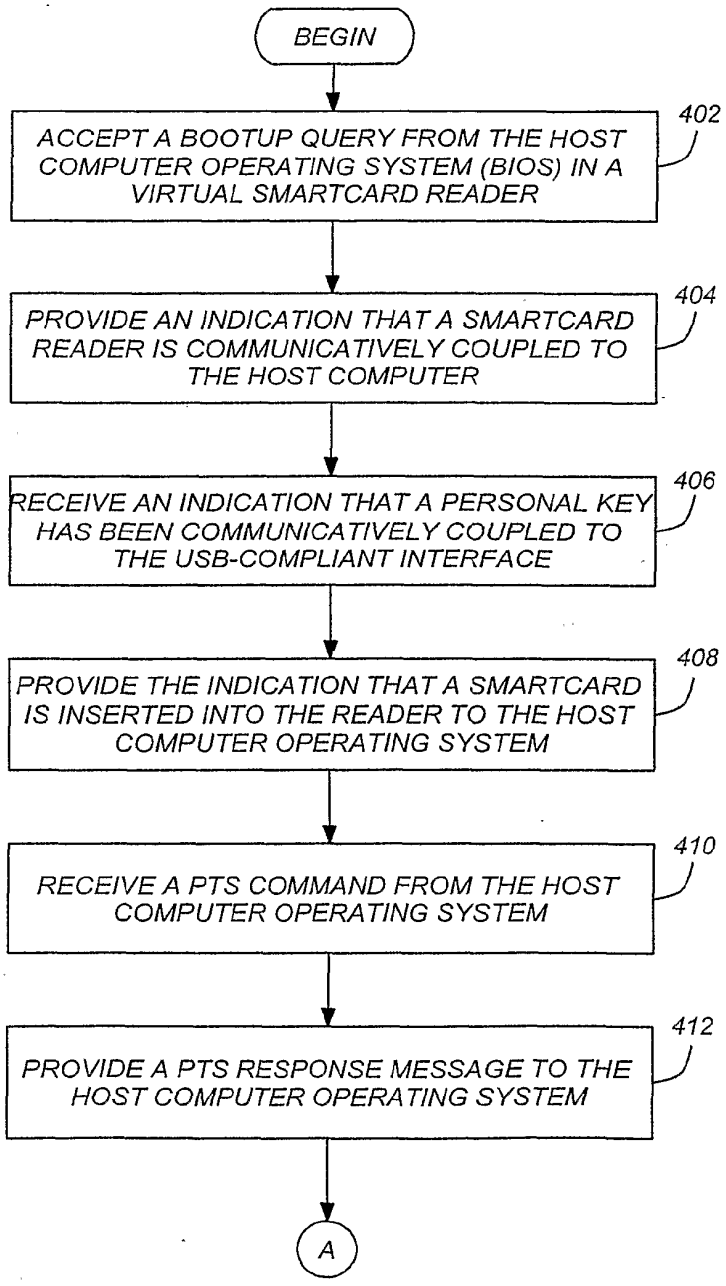

BEGIN
ACCEPT A BOOTUP QUERY FROM THE HOST COMPUTER OPERATING SYSTEM (BIOS) IN A VIRTUAL SMARTCARD READER
402
PROVIDE AN INDICATION THAT A SMARTCARD READER IS COMMUNICATIVELY COUPLED TO THE HOST COMPUTER
404
RECEIVE AN INDICATION THAT A PERSONAL KEY HAS BEEN COMMUNICATIVELY COUPLED TO THE USB-COMPLIANT INTERFACE
406
PROVIDE THE INDICATION THAT A SMARTCARD IS INSERTED INTO THE READER TO THE HOST COMPUTER OPERATING SYSTEM
408
RECEIVE A PTS COMMAND FROM THE HOST COMPUTER OPERATING SYSTEM
410
PROVIDE A PTS RESPONSE MESSAGE TO THE HOST COMPUTER OPERATING SYSTEM
412
A

FIG. 4A

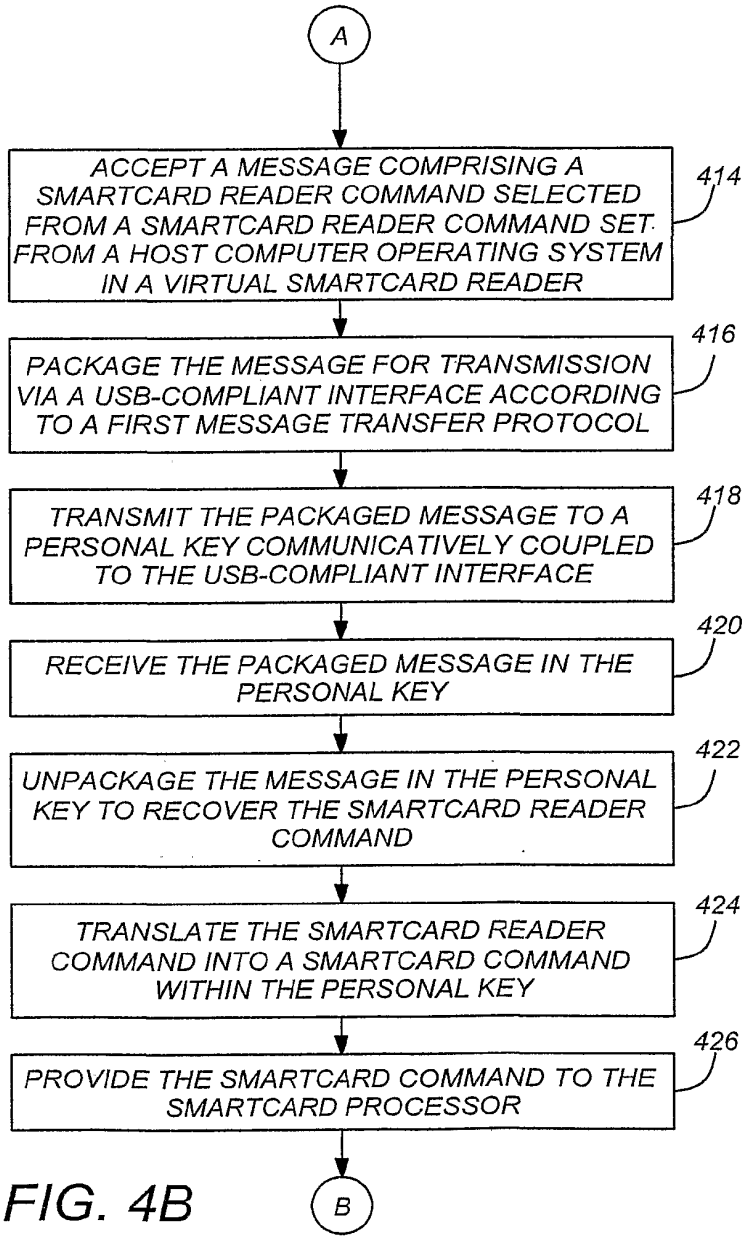

A
ACCEPT A MESSAGE COMPRISING A SMARTCARD READER COMMAND SELECTED FROM A SMARTCARD READER COMMAND SET FROM A HOST COMPUTER OPERATING SYSTEM IN A VIRTUAL SMARTCARD READER
414
PACKAGE THE MESSAGE FOR TRANSMISSION VIA A USB-COMPLIANT INTERFACE ACCORDING TO A FIRST MESSAGE TRANSFER PROTOCOL
416
TRANSMIT THE PACKAGED MESSAGE TO A PERSONAL KEY COMMUNICATIVELY COUPLED TO THE USB-COMPLIANT INTERFACE
418
RECEIVE THE PACKAGED MESSAGE IN THE PERSONAL KEY
420
UNPACKAGE THE MESSAGE IN THE PERSONAL KEY TO RECOVER THE SMARTCARD READER COMMAND
422
TRANSLATE THE SMARTCARD READER COMMAND INTO A SMARTCARD COMMAND WITHIN THE PERSONAL KEY
424
PROVIDE THE SMARTCARD COMMAND TO THE SMARTCARD PROCESSOR
426
B

FIG. 4B

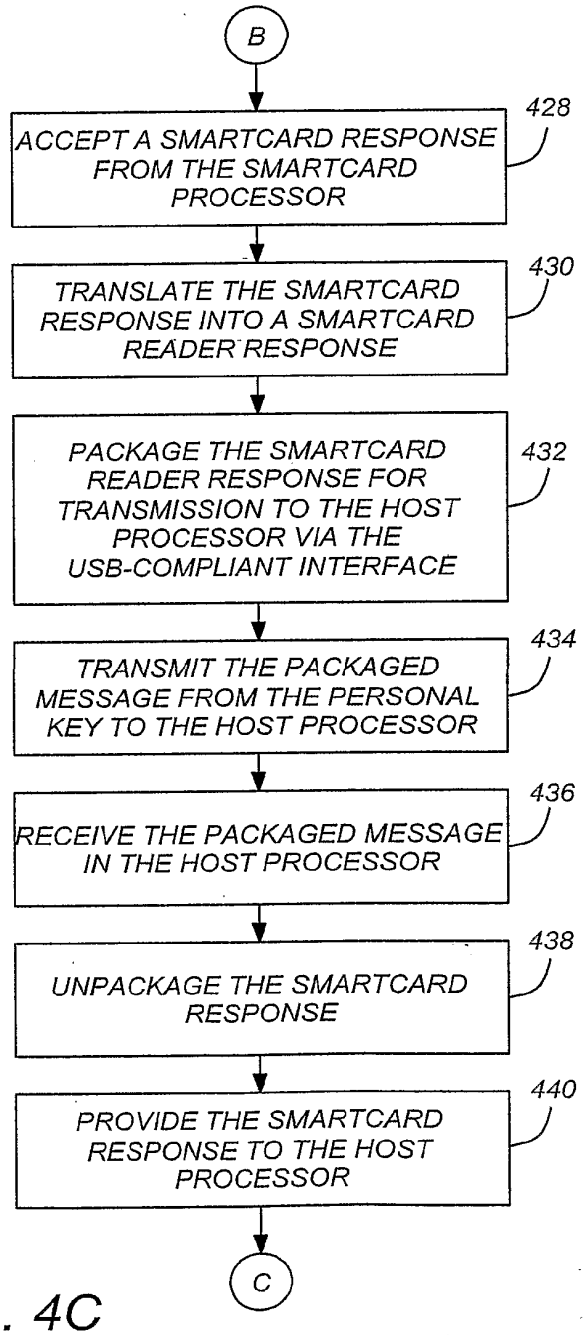

B
ACCEPT A SMARTCARD RESPONSE FROM THE SMARTCARD PROCESSOR
428
TRANSLATE THE SMARTCARD RESPONSE INTO A SMARTCARD READER RESPONSE
430
PACKAGE THE SMARTCARD READER RESPONSE FOR TRANSMISSION TO THE HOST PROCESSOR VIA THE USB-COMPLIANT INTERFACE
432
TRANSMIT THE PACKAGED MESSAGE FROM THE PERSONAL KEY TO THE HOST PROCESSOR
434
RECEIVE THE PACKAGED MESSAGE IN THE HOST PROCESSOR
436
UNPACKAGE THE SMARTCARD RESPONSE
438
PROVIDE THE SMARTCARD RESPONSE TO THE HOST PROCESSOR
440
C

FIG. 4C

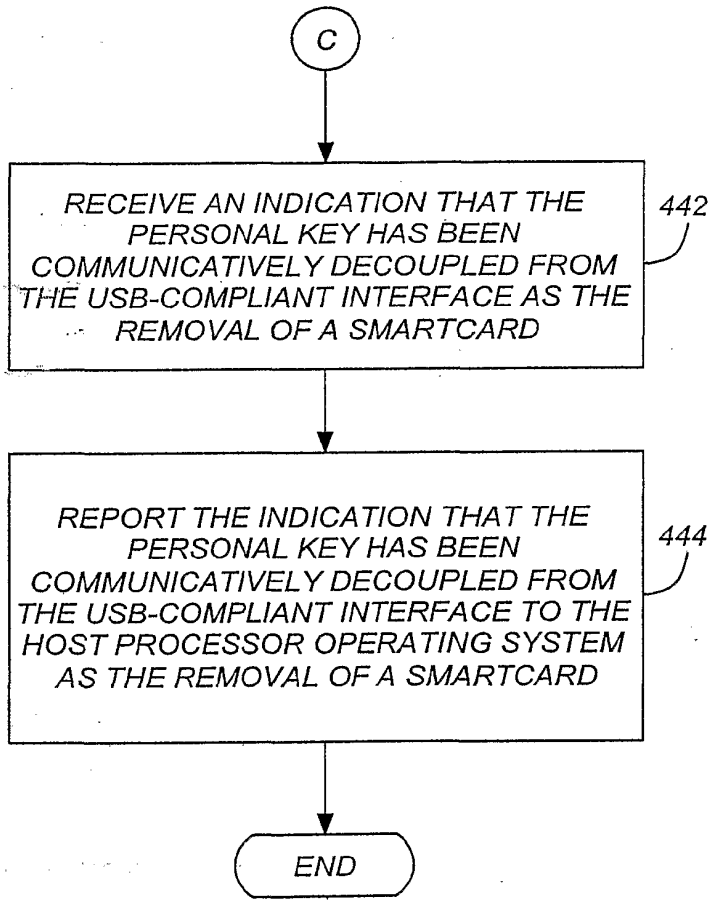

C
RECEIVE AN INDICATION THAT THE PERSONAL KEY HAS BEEN COMMUNICATIVELY DECOUPLED FROM THE USB-COMPLIANT INTERFACE AS THE REMOVAL OF A SMARTCARD
442
REPORT THE INDICATION THAT THE PERSONAL KEY HAS BEEN COMMUNICATIVELY DECOUPLED FROM THE USB-COMPLIANT INTERFACE TO THE HOST PROCESSOR OPERATING SYSTEM AS THE REMOVAL OF A SMARTCARD
444
END

FIG. 4D

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 February 2003 (20.02.2003)

PCT

(10) International Publication Number
WO 03/014887 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/EP02/08069

(22) International Filing Date: 18 July 2002 (18.07.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/924,502 9 August 2001 (09.08.2001) US

(71) Applicant: ACTIVCARD IRELAND, LIMITED [IE/IE]; -, 30 Herbert Street, Dublin 2 (IE).

(72) Inventor: HILLHOUSE, Robert, D.; -, Unit 4B, 120 Holland Avenue, Ottawa, Ontario K1Y0X6 (CA).

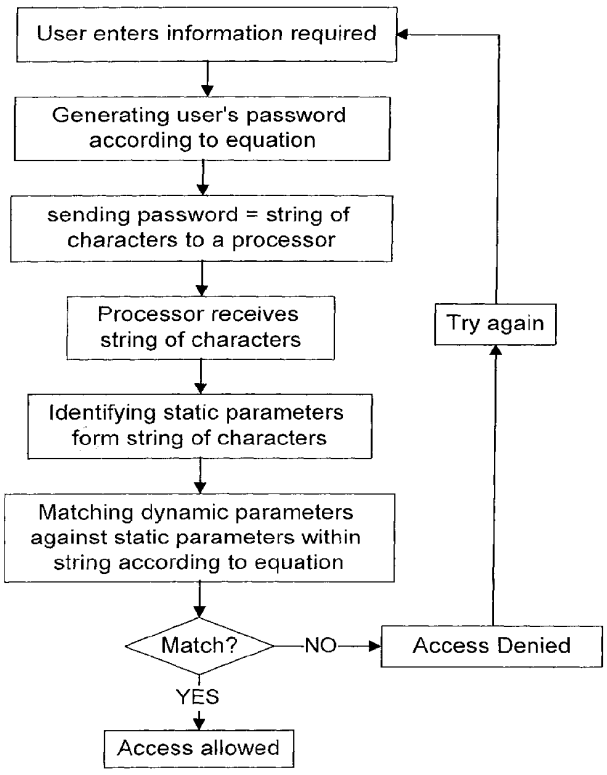
(74) Agent: CABINET JP COLAS; -, 37 avenue Franklin D. Roosevelt, F-75008 Paris (FR).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD FOR SUPPORTING DYNAMIC PASSWORD



(57) Abstract: A method of generating dynamic password is disclosed. A method of generating a dynamic password comprising the steps of providing a plurality of variable parameters, each parameter from the plurality of variable parameters being variable upon predetermined criteria; providing a plurality of predetermined static parameters; and processing at least some of the plurality of variable parameters and of the predetermined static parameters according to a dynamic password generating equation manipulating at least some of the plurality of variable parameters and of the predetermined static parameters resulting in an ordered sequence of dynamic and static parameters.

WO 03/014887 A2

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Method for Supporting Dynamic Password

[001] The present invention relates to a method of generating passwords and more particularly to a method of generating a password that changes as a function of various parameters making the password dynamic.

Background of the Invention

[002] Security is fast becoming an important issue. Is has always been an issue for everybody to protect his belongings. It is also well known that with the proliferation of computers and computer networks into all aspects of business and daily life - financial, medical, education, government, and communications - the concern over secure file access is growing. Using passwords is a common method of providing security. Password protection and/or combination type locks are employed for computer network security, automatic teller machines, telephone banking, calling cards, telephone answering services, houses, and safes. These systems generally require the knowledge of an entry code that has been selected by a user or has been preset.

[003] Preset codes are often forgotten, as users have no reliable method of remembering them. Writing down the codes and storing them in close proximity to an access control device (i.e., the combination lock) results in a secure access control system with a very insecure code. Alternatively, the nuisance of trying several code variations renders the access control system more of a problem than a solution.

[004] It is well known that a user determines a meaningful password, in the form of, for example, the name of their dog, the birth date of their child or an election year of the favorite candidate. This type of password is easily compromised with investigation. Conversely, a computer can randomly associates a password with a user, but this type of password is meaningless to the user and as such difficult to memorize. Consequently, the former method, which is simple, is insecure and the latter method, which is more secure, is difficult to use and often leads to a user writing their password next to their computer, thereby making the system insecure.

[005] The multiplicity of protected system encountered in the daily life of an individual renders the use of password particularly inconvenient, because a user has to remember a password for each accessible system. For example, the user must remember passwords for accessing network, database, E-mail, bank machine, personal

IPR2022-00412
Apple EX1053 Page 736

voice mails at home and at work, etc. The plurality of the systems wherein a password is needed favors a single simple password for all systems. In addition, a skilled person may find a predetermined password given sufficient time, rendering the system insecure. In more sophisticated theft situations, "Trojan horse" type viruses can be used to capture a user ID number and password that have been entered at a keyboard or across a network connection. That is, the user thinks he is logging on as usual, but the dialogue box in which the data is entered is really a look-alike window that is capturing his keystrokes.

[006] To secure access to a network, a further system was developed that relies on a user's personal information. A user requesting access to the network is prompted to answer a series of questions regarding his private life displayed on a computer screen. Such questions might be related to a relative's date of birth, a bone that was broken during childhood, a year of his first car accident, insurance company, address in January 1994, name of his first girlfriend, etc. The computer checks the validity of the answers before allowing access to the user. A computer is programmed with pertinent questions to ask a user and answers associated therewith, and when the system is initialised, the user enters the answers a first time, they are stored in a memory of the system, and are associated with the user identity. The time taken to answer all the questions prior to gaining access to the system is burdensome. It is evident that a major inconvenient with such a system is that a skilled person can find enough information of a personal nature relating to a user for answering properly the questions, and as such render the security ineffectual.

Object of the Invention

[007] To overcome such disadvantages, it is an object of this invention to provide a method for rendering a computer system access more secure.

[008] It is another object of this invention to provide a method for generating dynamic password.

[009] It is a further object of this invention to provide a method for generating a dynamic password dependent on various dynamic parameters.

Summary of the Invention

[0010] In accordance with a preferred embodiment of the present invention, there is provided a method of password verification comprising the steps of:

providing a process for transforming at least a variable parameter into an ordered string of characters, wherein the process sometimes results in different ordered strings of characters for a same variable parameter;

providing at least a variable parameter as a known password;

determining from data available to an individual and from the known password a static string;

providing the determined static string as a password for verification;

verifying the static string to determine that it is an accurate transformation of the at least a variable parameter according to the provided process and when the determination is that the transformation is accurate, providing an indication that the password is verified.

[0011] In accordance with another preferred embodiment of the present invention, there is provided a method of changing dynamic passwords comprising the steps of:

providing a string of characters, the string including indications of at least a parameter from a plurality of parameters, the at least a parameter being a variable parameter variable upon predetermined criteria;

receiving the provided string of characters; and,

storing data based on the known password, the data sufficient for verifying provided passwords to determine their accuracy.

[0012] Advantageously, the invention provides a method of verifying a dynamic password comprising the steps of:

receiving a password comprising a string of characters wherein the characters are sequenced according to a predetermined sequence of variable parameters and static parameters;

identifying static parameters within the string of characters;

IPR2022-00412
Apple EX1053 Page 738

determining dynamic parameter values related to the dynamic parameters in accordance with the predetermined sequence ;

comparing static parameters received within the string of characters with previously stored static parameters and the received dynamic parameter within the determined dynamic parameters to determine a first comparison result;

wherein upon both the first comparison result being indicative of a match, the dynamic password is validated.

Further advantageously, the invention provides a method of generating a dynamic password comprising the steps of:

providing a process for transforming at least a variable parameter into an ordered string of characters, wherein the process sometimes results in different ordered strings of characters for a same variable parameter; and,

providing at least a variable parameter as a password, the provided variable parameter provided by an individual via a data entry device.

Brief description of the drawings

[0013] Exemplary embodiments of the invention will now be described in conjunction with the following drawings, in which:

[0014] Fig. 1 is a computer screen display of a password dialog box;

[0015] Fig. 1a is an example of a filled password dialog box on a computer screen display;

[0016] Fig. 2 is a flow diagram of a method of evaluating a dynamic password generated according to the present invention;

[0017] Fig. 3 is an illustration of a computer screen displaying some possible images incorporated in the password;

Detailed Description of the Invention

[0018] In many large companies, the computer system is organized as a network to reduce the cost of purchasing and installing software on all the stations existing in the company. A main advantage of using a network is to facilitate data accessibility to each

employee. However, it is necessary to limit access of a company's network to the company's employees. As such, Fig. 1 is an example of a screen display prompting an employee to enter a login identity and an associated password to allow the employee to access the network. An example of a filled dialog box is shown in Fig. 1a. Classically, the login identity is the user's first name, illustrated here, as "Smith" and an exemplary password is "Fido", their dog's name. For security purpose, each character of the password is replaced with a star on the display so that nobody can read it. Each time a user is prompted to enter his password, the password is always identical to the one previously entered by the user unless the user has modified their password during a previous session. An ill-intentioned person can easily find out this type of static password and freely enter a company's network system.

[0019] Optionally, to make the system more difficult to break, the network system is organized in such a way that regularly all the employees are prompted to enter a new password. Often, the system allows the users to combine a non-determined number of letters, either small or capital, and digits in their passwords. However, due to the multiplicity of the systems and the recurrence of the demand, employees often use the same password to which a number is just added. For example, the "Fido" password becomes after a change request "Fido1". During the time period lasting between two successive modifications of a password, the password remains unchanged. A competent person may rapidly find out the password of a user and access a company's network..

[0020] As mentioned, the fact that the password remains unchanged during a long period of time between two modifications renders the system insecure. It will be advantageous to provide a security system based upon a dynamic password, i.e. a password comprising at least one parameter that changes in an uncontrollable way.

[0021] A most probable parameter that is uncontrollably variable is a parameter related to time. It is therefore advantageous to introduce a parameter related to the time in a dynamic password generation process because the time can be used in many ways such as hour of the day, day of the week/month, age, etc. By introducing at least a time parameter into a dynamic password generating equation, a password is automatically and deterministically different nearly every time it is used. The password mostly comprises some static or passive parameters such as the name of the user and perhaps

also isolated letters that may complicate the determination of the password. An example of such a dynamic password generating equation is shown below:

[0022] $hour + "Smith2" + $mday + 23 + "I" + ($hour + 16)/2

[0023] Where the uncontrollably variable parameters are:

hour that represents the hour of the day, and mday that represents the day of the month.

[0024] Where the static parameters are:

Smith2 that represents the user's name and can be easily remembered by the user and I is an isolated letter.

[0025] The dollar sign indicates a variable parameter, and the quote sign is indicative of static parameters. Alternatively, the distinction between static and variable parameters is made another way or using other characters.

[0026] Assuming that a user wants to access the company's network at 8:22 am on May 25, and has the account Smith, she determines from the variable password equation her password at the present time. Here it is:

8Smith248I12

[0027] and enters it into the system which verifies it. Anyone trapping the password and storing it for later use will be sadly disappointed because the password will expire one hour later while Smith easily determines the correct password an hour later without needing to change the password on the system.

[0028] Of course, the predetermined equation shown here is just for illustrative purpose. In the present example, only two different variable parameters are in the equation, there is no limitation as to the number of these parameters or as to the number of static parameters. However, it is most probably difficult to introduce too many parameters in a single equation, either variable or passive, because the user has to remember them and their combination, and as such has to memorize at least the order in which the various parameters have to be entered. Advantageously, the parameters variable and passive are not difficult to memorize because they are certainly available and easily accessible by the user such as the hour of the day, the date or a name, a word of the day, etc.

[0029] Referring now to Fig. 2, a flow diagram of a method of validating a dynamic password is illustrated. The user needs to know the equation for generating the dynamic password. In the present example the equation is:

$hour + "Smith2" + $mday + 23 + "I" + ($hour + 16)/2,

the user provides the hour of the day – "8" -, the characters "Smith2" followed by the value 48 being the day of the month plus 23, the letter "I" and 12 being (8+16)/2. The processor receives the string of characters for verifying the validity of the dynamic password. The processor generates a same password to verify that the user's password and then compares the characters within the string relative to the generated string according to the equation.

[0030] Eventually, a problem might rise when a password is entered at a time close to a change of the hour, for example. For example, assuming a variable parameter corresponds to the hour a user is entering a password, if the user's watch indicates 7:58 am, which is a time close to changing from 7 to 8, and the computer's watch has already turned over 8, the user might be rejected because the user password indicates a character 7 where the computer waits a 8. Even in these situations, it is easy for a user to either wait a few minutes or to realize that the system hour may be 7 or 8. Of course, synchronizing computers to the network password server clock will obviate this problem so long as users verify the time on their computers and not with their watches or desk clocks. Eventually, during a short period of time of a few minutes overlapping a change of hour as in the previous example, the network server accepts a password wherein the character indicative of the hour is incorrect within predetermined limits. In the previous example, the computer accepts password comprising the character 7 instead of 8 for indicating the hour. Similarly, if the user's watch indicates 8:02 am, and the computer's watch indicates 7:58 am, the computer accepts password comprising the character 8 instead of 7 for indicating the hour.

[0031] What may introduce a difficulty for a user are the numbers to memorize and eventually the operations to perform to complete the password. There are no prerequisites to incorporate operations in an equation for generating a dynamic password. Similarly, there is no prerequisite not to incorporate operations while

elaborating or programming the dynamic password generating equation for securing a network access.

[0032] In a further embodiment, the generation of a dynamic password relies again on a predetermined equation wherein an image is introduced as a parameter along with the variable and the static parameters. Referring to Fig. 3, a computer screen is displaying a plurality of images including various shapes, animals, trees, and different symbols. An image of a series as the one illustrated in Fig. 3 is part of a dynamic password generating equation. An example of such a dynamic password generating equation is shown below:

$hour + "Smith2" + $image

Where the variable parameter is: hour that represents the time of the day.

Where the static parameter is: Smith2 - the user's name.

Where the image parameter is: image

[0033] Where the dollar sign indicates a variable parameter, the quote sign is indicative of a static parameter.

[0034] Assuming that the user wants to access her company's network at 8:22 am. An image is presented in the dialogue box asking for her password. For example, a tree may be displayed. In that instance, the user enters a password according to the above-predetermined dynamic password generating equation. The password will thus be in the form of:

8Smith2tree

[0035] Advantageously, an interpretation of the image is as valid as the image itself. For example, if the imaged tree is a pine, the password might reflect this particularity and incorporate the tree species. Moreover, English is not the exclusive language that can be used to describe a tree. Indeed, computers of large companies, especially international companies, are preferably programmed to accept passwords generated in any of a number of possible languages. Alternatively, only the user's mother tongue is accepted for a given password entry. Consequently, incorporating an image in the equation allows multiple other possibilities for the resulting password.

[0036] Back to the previous example and the possibilities allowed with a single image of a tree, here are 3 of the possible passwords:

8Smith2tree

8Smith2pine

8Smith2arbre

[0037] All the images are interpreted to a certain extent. For example, if an image of a bulb is selected, the possible words illustrating a bulb, not withstanding a foreign language, might be lamp, idea, light, lightbulb, bulb, eureka, etc. Of course the flexibility in image identification is a parameter that is set during system implementation or alternatively as an option to be set by a system administrator.

[0038] Thus, generating a dynamic password incorporating an image in the equation along with the variable and the static parameters also makes the system less secure when variability of many parameters is supported. That said, since the image is not immediately discernible to an unauthorized individual and its location within the password is unknown, it is believed that overall security will increase when the system is used by unconcerned individuals – individuals who are not specially trained in computer security.

[0039] In the example shown here, only one variable, one static, and one image parameter form part of the predetermined equation for generating the password but of course, there is no limitation as to the number of these parameters. The limit that may be taken into consideration is the good will of the user as to his capacity to memorize parameters to enter when prompt to do so. Additionally, there is no prerequisite to incorporate operations in the equation for generating a dynamic password. Similarly, there is no prerequisite not to incorporate operations while elaborating or programming the dynamic password generating equation for securing a network access.

[0040] Even though a dynamic password offers enormous advantages over static passwords, it is beneficial to have the possibility to change the password from time to time to decrease drastically the possibility to compromise security of the system. A way to achieve such beneficial possibility is to assign a code to the different parameters that compose a dynamic password. A code might be of various forms as for example an

Arabic number, or a Roman numeral, or a letter, etc. The codes are assigned, for example, according to a predetermined setting or more probably are randomly assigned.

[0041] Referring to a previous example wherein the dynamic password generating equation was in the form of:

$hour + "name2" + $image

[0042] A first possibility is to determine as many codes as parameters in the equation. So in the present example, three codes are assigned:

Possibility 1	Possibility 2	Possibility 3
code 1 → hour	code 1 → name	code 1 → image
code 2 → name	code 2 → image	code 2 → hour
code 3 → image	code 3 → hour	code 3 → name
Possibility 4	Possibility 5	Possibility 6
code 1 → hour	code 1 → name	code 1 → image
code 2 → image	code 2 → hour	code 2 → name
code 3 → name	code 3 → image	code 3 → hour

[0043] An advantage in coupling codes to parameters is that the codes can be ordered arbitrarily by the server, allowing for a multiplicity of representations of a same password. Thus, intercepting the password equation is of limited value. Also, often codes are easier to enter than textual representations of parameters. Effectively, by changing the code assignment, the password though unchanged, appears differently to a Trojan Horse application and is therefore more difficult to decode. Also, it is unclear what each code entry refers to. Here, there exist 6 possibilities of reassigning the three codes to the three parameters, which leads to six different possible password entries resulting in the three identical parameters in the same sequence as in the Possibility 1.

[0044] To drastically increase the password's possibilities wherein the same dynamic and static parameters are initially required, the number of codes can exceed the number of parameters. For example, if 10 codes are available and 5 parameters are required for generating a dynamic password, the number of possibilities is increased according to the combination of 5 codes chosen from 10 to obtain an arrangement of the

parameters identical to the arrangement required in the equation. Consequently, the number of possibilities is increased by about 252. Of course, these numbers are cited for exemplary purpose only, the number of codes available is not limited to any of the mentioned numbers.

[0045] Static parameters as used in the specification denote parameters that do not change. These can include string values and defined answers to questions that do not change. For example, "iQw4" is a string. Another static parameter is a user's name, employee number, address, etc. Which are determined and unchanging parameters. Of course, the static parameters can also be identified within passwords by encoded value in order to make interception of the password during password changes more difficult.

[0046] When a system has access to a significant amount of data, it is also possible to relate the password to data known to the system. Some example variable parameters include: days to a new moon, days until a product release, days since year end, months since hiring, years since hiring, employee age in years, months since last vacation week, number of people on vacation within a person's group, amount on last paycheck, taxes deducted on last paycheck, amount in employee savings plan, and so forth. Also, posted data is useful such as today's lunch menu items, word of the day, and so forth.

[0047] In order to verify a password when provided, there are several possible methods. According to a preferred embodiment, the static portions of the password are hashed either separately or in a concatenated or other joined form. The hashed value is stored. When a password is received, it is separated into static and dynamic values. The dynamic values are regenerated to verify the dynamic values. The static values are hashed and the hash values are compared. As such, the resulting static portions are not stored on the server and cannot be detected by a snooping device. The dynamic parameters are stored in an encoded fashion that is typically other than human intelligible. For example, if 256 variable parameters are known, the variable parameters are stored as 8 bit values.

[0048] Alternatively, the dynamic values are verified without regenerating same. For example, if the variable parameter is day of month + 23, then the verification process merely subtracts 23 from the provided value and compares the result to the

present day of the month. Of course, other methods of password verification are possible.

[0049] Advantageously, the dual composition of these passwords, i.e. dynamic and static values renders the dynamic passwords usable with various existing system without requiring any other support. Typically, a password is used for activating encryption keys for encrypting data. Advantageously, the static values of a dynamic password are used as keys like typical passwords. However, the presence of dynamic values in combination with the static values in a dynamic password increases the security of the system. That said, even if static values are potentially accessible to an unauthorized individual, their location within the password is unknown. Therefore, accessibility to encryption data is possible thanks to the static values and moreover, the accessibility is protected by the dynamic values.

[0050] Numerous other embodiments might be envisioned without departing from the scope and the spirit of the present invention. For example, the description of the invention implicitly inferred that the dynamic password generating equation was identical for all the employees of a company. The difference between the dynamic passwords of two employees login in at the same time being the static parameters. However, each employee can have a specific dynamic password generating equation. The multiplicity of equations, i.e. as many equations as employees, might be advantageous if an employee leaves the company. In such a case, the equation is deleted and nobody else in the company is affected, otherwise, the whole system must adapt to the departure for keeping the system as secure as possible.

Claims

What is claimed is:

1. A method of password verification comprising the steps of:

providing a process for transforming at least a variable parameter into an ordered string of characters, wherein the process sometimes results in different ordered strings of characters for a same variable parameter;

providing at least a variable parameter as a known password;

determining from data available to an individual and from the known password a static string;

providing the determined static string as a password for verification; and,

verifying the static string to determine that it is an accurate transformation of the at least a variable parameter according to the provided process and when the determination is that the transformation is accurate, providing an indication that the password is verified.

2. A method according to claim 1, characterized in that the step of verifying the static string includes the steps of:

performing the process for transforming at least a variable parameter on the known password to determine a second static string;

comparing the provided static string with the second static string to determine a comparison result and,

when the comparison result is indicative of a match, providing an indication that the password is verified.

3. A method according to claim 1, characterized in that the at least a variable parameter includes an uncontrollably variable parameter.

4. A method according to claim 2, characterized in that the at least a variable parameter includes at least a static parameter.

IPR2022-00412
Apple EX1053 Page 748

5. A method according to claim 1, characterized in that the process includes steps of determining from present time data, a current value for a variable parameter relating to time.

6. A method according to claim 1, characterized in that the process includes steps of providing data to a user for interpretation by the user and then comparing the user's interpretation to a predetermined known interpretation.

7. A method according to claim 6, characterized in that the provided data is an image and the interpretation is a string indicative of the image.

8. A method according to claim 1, characterized in that the known password is provided by a user.

9. A method according to claim 8, characterized in that the known password is entered as a string of characters and wherein at least a character is indicative of one of a variable parameter and a static parameter.

10. A method according to claim 9, characterized in that the string of characters is parsable to form the known password, the parsing distinguishing variable parameters from static parameters within the known password.

11. A method of changing dynamic passwords comprising the steps of:

providing a string of characters, the string including indications of at least a parameter from a plurality of parameters, the at least a parameter being a variable parameter variable upon predetermined criteria;

receiving the provided string of characters; and,

storing data based on the known password, the data sufficient for verifying provided passwords to determine their accuracy.

12. A method of changing dynamic passwords according to claim 11, comprising the step of:

IPR2022-00412
Apple EX1053 Page 749

with a processor parsing the provided string of characters to distinguish static data from the at least a variable parameter.

13. A method of changing dynamic passwords according to claim 11, characterized in that the parameters are selected from a plurality of available parameters and characterized in that the plurality of available parameters are provided to a user for selecting thereform.

14. A method of changing dynamic passwords according to claim 13, characterized in that the plurality of available parameters are each represented by an identifier and characterized in that the identifier for a given parameter in one instant is different from the identifier for a same parameter in another instant.

15. A method of changing dynamic passwords according to claim 11, characterized in that the step of storing data based on the known password comprises the steps of:

extracting static data from the known password;

hashing the extracted static data to determine at least a static hash value;

storing the at least a static hash value; and,

extracting dynamic data from the known password and storing indications of the dynamic data.

16. A method of verifying a dynamic password comprising the steps of:

receiving a password comprising a string of characters wherein the characters are sequenced according to a predetermined sequence of variable parameters and static parameters;

identifying static parameters within the string of characters;

determining dynamic parameter values related to the dynamic parameters in accordance with the predetermined sequence ;

comparing static parameters received within the string of characters with previously stored static parameters and the received dynamic parameter within the determined dynamic parameters to determine a first comparison result;

wherein upon both the first comparison result being indicative of a match, the dynamic password is validated.

17. A method of generating a dynamic password comprising the steps of:

providing a process for transforming at least a variable parameter into an ordered string of characters, wherein the process sometimes results in different ordered strings of characters for a same variable parameter; and,

providing at least a variable parameter as a password, the provided variable parameter provided by an individual via a data entry device.

18. A method of generating dynamic passwords according to claim 17, characterized in that the plurality of variable parameters comprises uncontrollably varying parameters.

19. A method of generating dynamic passwords according to claim 18, characterized in that the predetermined criteria for varying the variable parameters is characteristic of a time frame.

Fig. 1

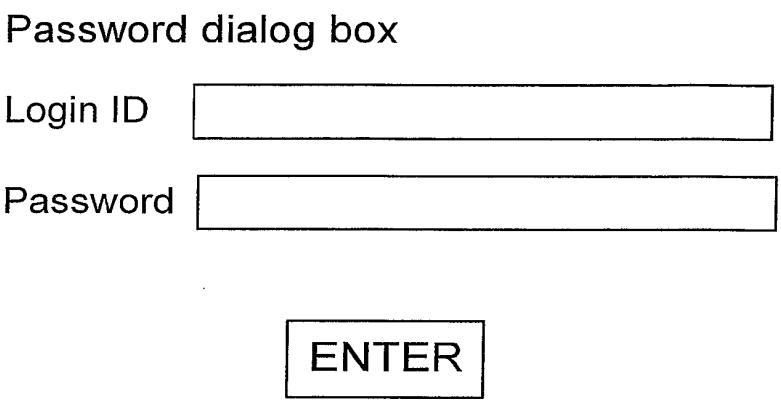
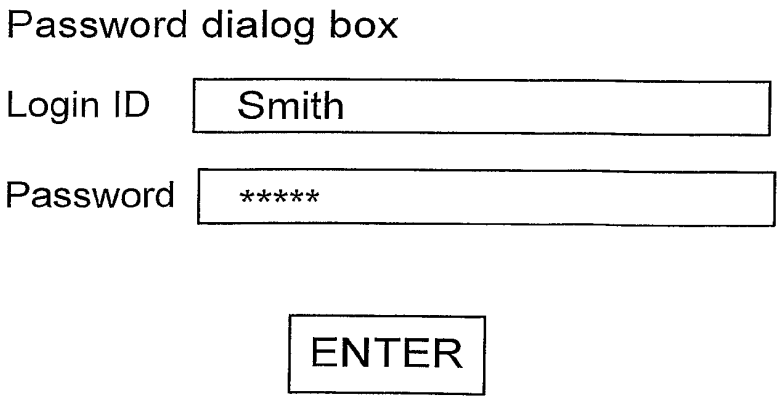

Password dialog box
Login ID
Password
ENTER

Fig. 1a


Password dialog box
Login ID
Smith
Password
*****
ENTER

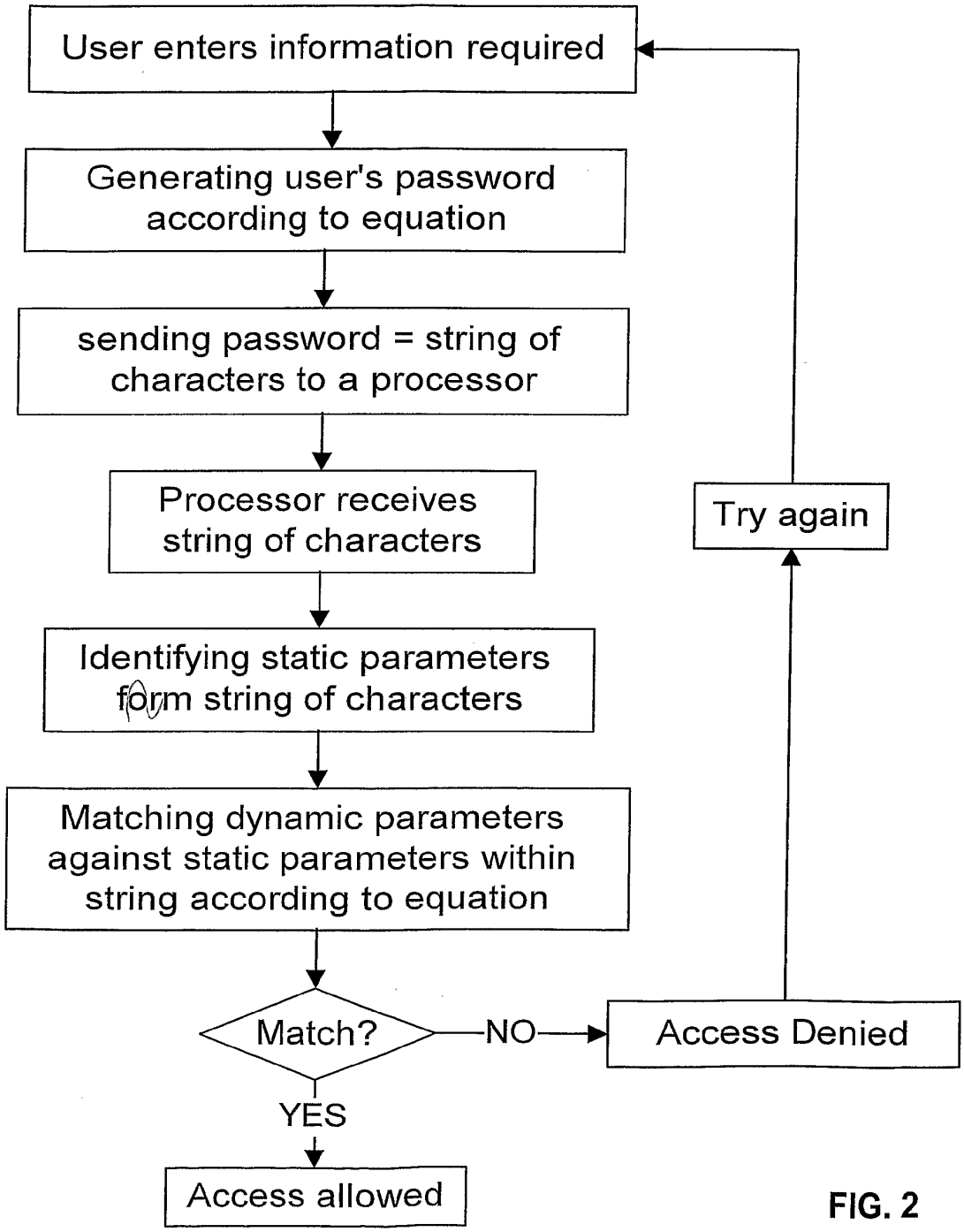

User enters information required
Generating user's password according to equation
sending password = string of characters to a processor
Processor receives string of characters
Identifying static parameters form string of characters
Matching dynamic parameters against static parameters within string according to equation
Match?
NO
Access Denied
Try again
YES
Access allowed

FIG. 2

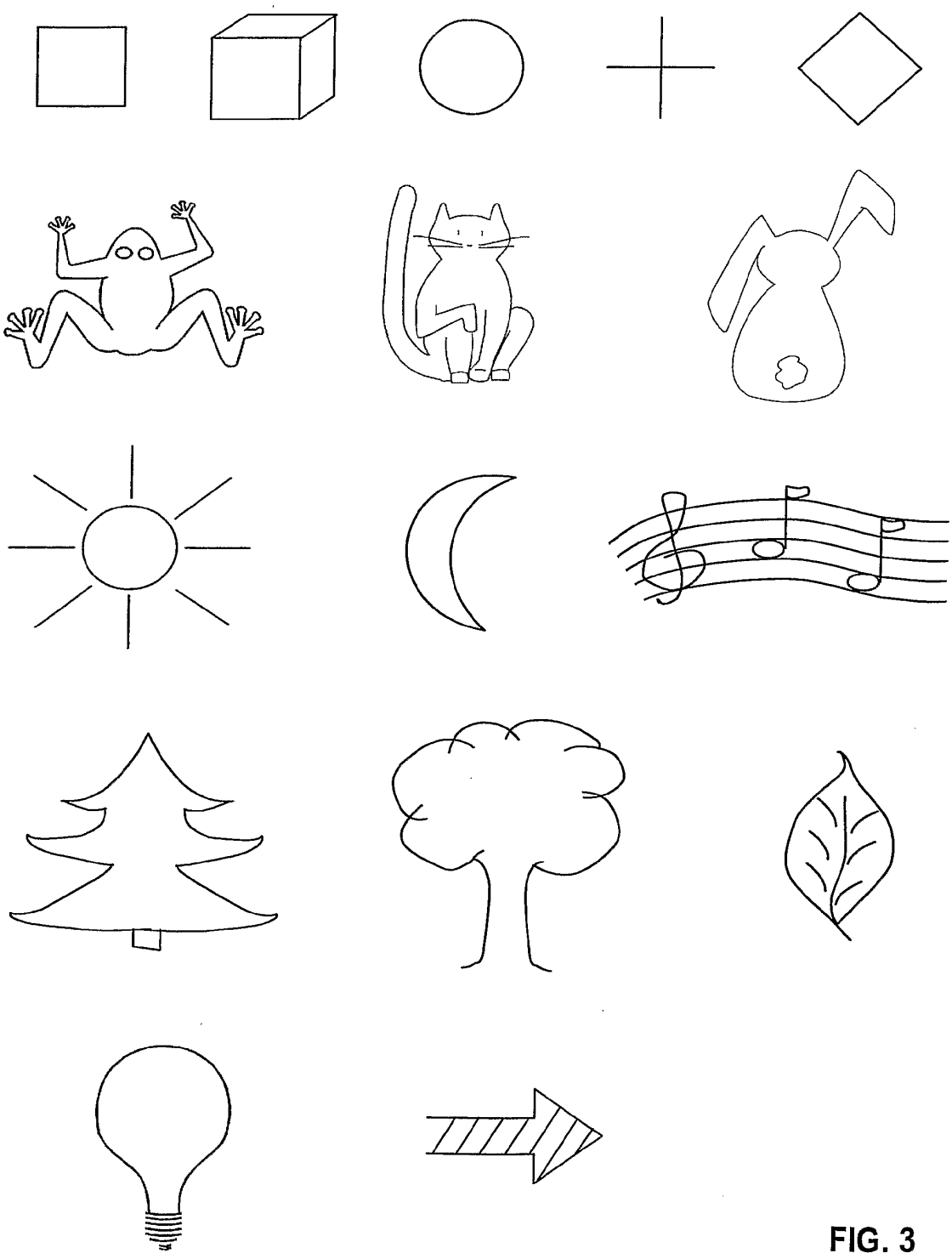


FIG. 3

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 April 2003 (24.04.2003)

PCT

(10) International Publication Number
WO 03/034189 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/EP02/11445

(22) International Filing Date: 11 October 2002 (11.10.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/977,202 16 October 2001 (16.10.2001) US

(71) Applicant: ACTIVCARD IRELAND, LIMITED [IE/IE]; 30 Herbert Street, 2 DUBLIN (IE).

(72) Inventor: CHARBONNEAU, Marc; 23, Terrace Sauve, Casselman, OTTAWA, Ontario KOA 1MO (CA).

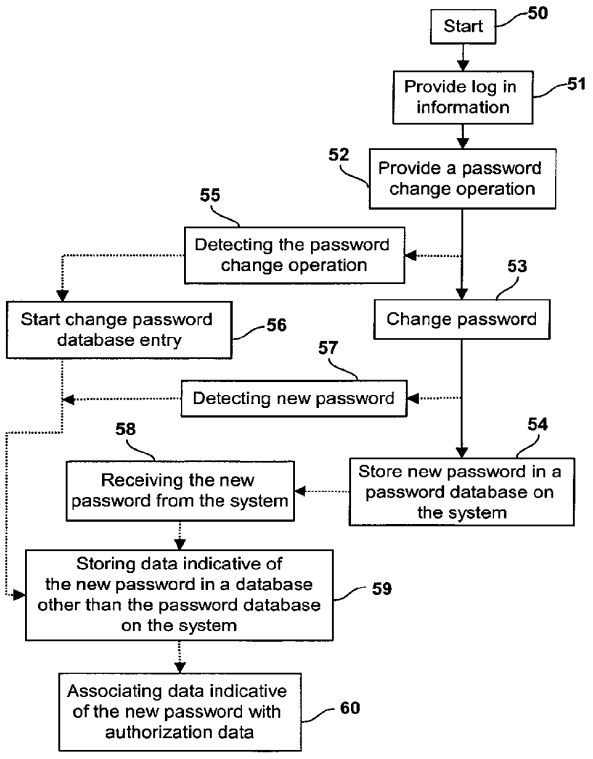
(74) Agent: CABINET JP COLAS; 37, avenue Franklin D. Roosevelt, F-75008 PARIS (FR).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD FOR SUPPORTING SINGLE SIGN ON



(57) Abstract: A method of securely supporting password change is disclosed. The method comprises the steps of: detecting an occurrence of a password change operation (55) in execution on a system and receiving a new password by the system; detecting the new password when provided (57); storing data indicative (59) of the new password in a database other than the password database of the system for later retrieval, the data indicative of the new password for provision to the system.

WO 03/034189 A2

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Method for Supporting Single Sign On

[001] The present invention relates to a method for changing password data, and more particularly, to a method for securely supporting password change for a central database of passwords independent of some processes with which the password is associated.

Background of the invention

[002] Security is fast becoming an important issue. It is well known that with the proliferation of computers and computer networks into all aspects of business and daily life - financial, medical, education, government, and communications - the concern over secure file access is growing. Using passwords is a common method of providing security. Password protection and/or combination type locks are employed for computer network security, automatic teller machines, telephone banking, calling cards, telephone answering services, houses, and safes. These systems generally require the knowledge of an entry code that has been selected by a user or has been preset.

[003] In many large companies, the computer system is organized as a network to reduce the cost of purchasing and installing software on all the stations existing in the company. A main advantage of using a network is to facilitate data accessibility to each employee. However, it is necessary to limit access of a company's network to the company's employees. As such, prior to access the company's network, a password window prompted the company's employees to enter a login identity and an associated password. Usually, a user specifies passwords. Most users, being unsophisticated users of security systems, classically choose as the login identity their first name, and their dog's name as a password for example. Each time a user is prompted to enter his password, the password is always identical to the one previously entered by the user unless the user has modified his password during a previous session. As such, many password systems are easily accessed through a simple trial and error process.

[004] Optionally, to make the system more difficult to break, the network system is organized in such a way that regularly all the employees are prompted to change their

password, or are required to run a specific routine to change their password. Often, the system allows the users to combine a non-determined number of letters, either small or capital, and digits in their passwords. During the time period lasting between two successive modifications of a password, the password remains unchanged. A competent person may rapidly find out the password of a user and access a company's network.

[005] Optionally, a password is stored in a password database and user authorisation information such as biometric information, a digital key, a smart card, or a global password is required to retrieve the password. When the password is retrieved, it is provided to the password window. It is known to those skilled in the art that a biometric identification system accepts unique biometric information from a user and identifies the user by matching the information against information belonging to registered users of the system. Fingerprint sensing and matching is a reliable technique for personal identification and/or verification.

[006] The combination of a password and biometric information such as a fingerprint for example is beneficial because it increases the security and limits accessibility to a system. However, an association between a biometric information sample and a password also raises a problem when the password is changed. If an individual changes his password manually using, for example, a change password command of a password protected system, a next time he wants to access the system and provides his fingerprint, his old password is retrieved and provided to the password prompt. The old password is not current and therefore a message indicating that the password is incorrect is provided for the user. Thus, the user has to manually type in the new password. Eventually, the user can run a password change routine wherein the old password is provided along with the fingerprint, the new password typed in and the biometric sample assigned from then to the new password.

Object of the Invention

[007] To overcome such an inconvenience, it is an object of this invention to provide a method for automatically assigning a new password.

[008] It is another object of the present invention to provide a method of detecting a password change operation in a system and prompt for a new password.

[009] It is another object of the present invention to provide a method of detecting a password change command and authorizing a password change operation.

Summary of the invention

[0010] In accordance with the present invention, there is provided a method of securely supporting password change comprising the steps of: detecting at least one of the operations in execution on a system comprising: detecting a password change operation, and detecting a new password storage operation; performing an operation to change the password of a user to a new password in the system; storing the new password in a password database on the system; and storing data indicative of a new password for later retrieval of the new password by the system in a database independent of the change password operation and of the database where the new password is stored .

[0011] In accordance with another embodiment of the present invention, there is provided a method of securely supporting password change comprising the steps of: detecting a password change operation in execution on a system; displaying to a user a prompt for a new password, the prompt independent of the password change operation; receiving the new password; performing an operation to change the password of a user to a new password in the system; storing the new password in a password database on the system; and storing data indicative of a new password for later retrieval of the new password by the system in a database independent of the change password operation and of the database where the new password is stored..

[0012] In accordance with another embodiment of the present invention, there is provided a method of securely supporting password change comprising the steps of: detecting a password change operation in execution on a system; displaying to a user a prompt for authentication information, the prompt independent of the password change operation; receiving the authentication information; when the authentication information is indicative of a known user, providing a password associated with the user to the system; performing an operation to change the password of a user to a new password in the system; storing the new password in a password database on the system; and storing data indicative of a new password for later retrieval of the new

password by the system in a database independent of the change password operation and of the database where the new password is stored .

[0013] In accordance with another preferred embodiment of the present invention, there is provided a method of securely supporting password change comprising the steps of: detecting a password change operation in execution on a system; performing an operation to change the password of a user to a new password in the system; storing the new password in a password database on the system; and storing data indicative of a new password for later retrieval of the new password by the system in a database independent of the change password operation and of the database where the new password is stored; wherein the system has a known user authorized thereon, and wherein the step of performing an operation to change the password comprises the step of automatically generating a new password.

Brief description of the drawings

[0014] Exemplary embodiments of the invention will now be described in conjunction with the following drawings, in which:

[0015] **Fig. 1** is a flow diagram of a prior art method of associating a password to a fingerprint upon a match of a fingerprint with an associated template;

[0016] **Fig. 2** is an example of a prior art password window dialog display;

[0017] **Fig. 2a** is an example of a filled password window dialog box on a computer screen display;

[0018] **Fig. 3** is a flow diagram of a prior art method of changing password;

[0019] **Fig. 4** is a flow diagram of a prior art method of retrieving the password for provision to the system;

[0020] **Fig. 5** is a flow diagram of a method of securely supporting password change in accordance with a preferred embodiment of the present invention;

[0021] **Fig. 6** is a flow diagram of a method of securely supporting password change in accordance with another preferred embodiment of the present invention;

[0022] **Fig. 7** is a flow diagram of a method of securely supporting password change in accordance with another preferred embodiment of the present invention; and,

[0023] **Fig. 8** is a flow diagram of a method of securely supporting password change in accordance with another preferred embodiment of the present invention wherein a choice is given to the user.

Detailed description of the invention

[0024] In the prior art, many security systems involving imaging fingerprints to allow access for example to a building, to a specific area within a building, to a computer, are described. The security systems wherein biometric information is used for identifying and authorizing access to an individual mostly rely on a prior art method as shown in Fig.1. Following a starting step 10, after a biometric information sample, in a form of a fingerprint for example, has been provided to a system at step 11, in order to generate a fingerprint, a fingertip is imaged to generate an image thereof, which is called a fingerprint or a fingerprint image. The fingerprint is then characterized at step 12. During the process of identification, the characterized fingerprint is compared to stored templates associated with fingerprints of the person at step 13 – for a one-to-one identification system - or of any person registered for access the system – in a one-to-many identification system. Upon a positive result of the comparison, when there is a match between the provided fingerprint and a stored template associated with a fingerprint at step 14, the system provides at step 15 a password associated with the stored template to, for example, a legacy password based system and the user is identified and authorized at step 16.

[0025] Referring to Fig. 2, an example of a screen display prompting an employee to enter a login identity in 21 and an associated password in 22 to allow the employee to access the network. An example of the display of Figure 1 filled in is shown in Fig. 2a. Classically, the login identity is the user's name, illustrated here, as "Smith" in 23. For security purpose, each character of the password is replaced with a star on the display so that nobody can read it as shown in 24. Each time a user is prompted to enter his password, the password is always identical to the one previously entered by the user unless the user has changed his password during a previous session.

[0026] Optionally, to make the system more difficult to break, the network system is organized in such a way that, regularly, all the employees are prompted to enter a new password in order to change the passwords at regular intervals. Often, the system allows the users to combine a non-predetermined number of letters, either small or capital, and digits in their passwords. Referring to Fig. 3, a prior art method of changing passwords is shown. After a starting step 30, in order to access a system at step 32, the password change window prompts a user to provide an identity and the old password associated with the provided identity at step 31. Once authorized, the user is able to provide the system with a new password at step 33. Typically, the user is prompted to type in a new password two times as shown at step 34. The new password is stored in a password database of an application or operating system related to the password change operation on the system and now replaces the old password at step 35 before an ending session at 36.

[0027] Referring now to Fig. 4, a flow diagram of a method of retrieving the password for provision to the system is shown. For accessing a system after a starting step 40, a user provides authorization data at step 41, in the form of biometric information sample or information stored on a smart card. The authorization data is verified and is used to retrieve data indicative of the user password at step 42. Upon provision of the authorization data, the password is retrieved from a database other than the password database of the system or application at step 43 and provided to the system or application so that the user can gain access thereto.

[0028] The authorization data permits identifying a user based on, for example, biometric information provided therefrom. This provides an indication that the correct person was actually present when the request for changing a password was provided. A major advantage of using biometric information for retrieving a password is that the password does not have to be memorized. Typically, the user provides biometric information from a biometric source. The biometric information is characterized, processed and compared against templates stored in the system. Upon a match of the features extracted from the templates and the characterized biometric information corresponding to the biometric source provided by the user, an authorization signal is either provided or denied.

[0029] Referring now to Fig. 5, a method for securely supporting password change in accordance with a preferred embodiment is shown. To facilitate the comprehension of the figure, lines are plain for showing a classic password change routine flow, whereas dashed lines show changes in process flow for securely supporting password change. Each individual also has access from its workstation to a password change command. It is understandable that when a user has any doubt concerning the confidentiality of his password, he can change it independently of a network administrator. The user accesses the system at step 50 and provides a command 51 for a password change operation to be performed on the system at step 52. Usually, the user is prompted to type in a new password twice as disclosed with reference to Fig. 3 at step 53, and then the new password is stored in a password database on the system at step 54. Inconveniently, the password is changed independently of the authorization data or log in information when the system supports user authorization and password retrieval as disclosed with reference to Fig. 4. Therefore, the next time the user tries to access the system, his password information will not match with the new password – it has not been updated, and access will be denied.

[0030] According to the present invention, when a change password operation in execution on the system occurs, it is detected at step 55. That said, any password change command options in the form for example of the word "password" or the abbreviation "pwd" typed in are recognized. Of course, though it is preferred that all possible password change operations are detected, the present invention is advantageous if even a single change password operation is detected. The new password is changed at step 53 and the new password is stored in the password database on the system at step 54. Approximately simultaneously, the new password is detected by another process at step 57 that uses the detected data to change the password in another database at step 59. For example, the data indicative of the new password is automatically associated with the authorization data within a system at step 60 such as that of Fig. 4. Therefore, for future accesses to the system, the user just provides his authorization data in a form of a fingerprint for example, the system retrieves the data indicative of the new password associated with the authorization data and the user is authorized to access the system.

[0031] Alternatively, the storage of the new password in a password database on the system is detected and data indicative of the new password are also detected for storing in a database other than the password database on the system as shown at step 58.

[0032] Interestingly, the user is not aware of the detection procedure and of the automatic assignment of the authorization data to the data indicative of the new password. Therefore, the user types in a new password twice for storing the new password in a password database on the system, data indicative of the new password is saved in a database other than the password database on the system at step 59 and the password is changed on the system, and the user does not have to retype this new password for further access. However, because of the transparency of such a system, the user does not know whether his new password has effectively been changed or not.

[0033] Referring now to Fig. 6, a flow diagram of a method of securely supporting password change in accordance with another preferred embodiment of the present invention is shown. When a password change operation is provided at step 61, the password change operation is detected at step 61 and a secure password change process prompts the user for a new password at step 63 to allow the change password operation to proceed at step 64. The new password is provided to the process at step 65 to allow changing of the password, which is stored in an independent database at step 66. The data indicative of the new password is automatically associated with the authorization data in replacement of the data indicative of the old password. From the independent database, the new password is provided to a password database on the system at step 67 to change the password there. The prompt for a new password by the secure password change process instead of by the process associated with the system or application notifies the user that the password change operation has been detected and that the new password is accurately stored.

[0034] Advantageously, the above process is implemented with no apparent change to the users of the system. In other words, a user is completely unaffected by the method of Fig. 6, since it is transparent to the user and does not affect any existing change password processes.

[0035] Referring now to Fig. 7, a flow diagram of a method of securely supporting password change in accordance with another preferred embodiment of the present invention is shown. When a password change operation is provided at step 70, the password change operation is detected at step 71 and a secure user authorization process prompts the user for an authorization data at step 72. Once authorized at step 73, the system allows the change password operation to proceed at step 74. The new password is provided to allow changing of the password, which is stored in an independent database at step 75. The data indicative of the new password is automatically associated with the user identity in replacement of the data indicative of the old password. From the independent database, the new password is provided to a password database on the system at step 76 to change the password there. The prompt for user authorization data by the secure authorization process instead of by the process associated with the system or application notifies the user that the password change operation has been detected and that the new password is accurately stored.

[0036] The above process is highly advantageous. It provides a single password change process and as such a single ergonomic interface for changing passwords. Therefore, design and implementation of the secure change password process replaces all legacy change password processes allowing for better information for the users and a more modern and ergonomic process.

[0037] Further advantageously, the above process allows for changing of passwords of several systems/files/applications simultaneously. Thus, a single change password operation is used where before several or several hundred processes would have been required. This is most applicable when changing a password used to protect a single file such as a Microsoft ® Word® file or the like.

[0038] Of course, it is evident to those of skill in the art that a password entered in accordance with the above described process is optionally long and complex since there is no need to remember the password. Because of the automatic password retrieval, a user never needs to know their password so an arbitrary string of characters such as "efkjhgbshgdxfbkj#$$JHYT$kjsfd*(&REW^kvhgfd)(*^*&^%C^Tvc hbjhf86%(%(ffgf nm.b.nm.,mn.vb2609" is usable as a password allowing for greatly increased security.

[0039] Another advantage to the present method is that it allows tracking of old passwords to provide for access to older system restorations or old files that were saved using earlier passwords.

[0040] Of course, the process also supports different passwords for different systems, files and applications without substantial user inconvenience. This is achieved by storing each password in association with data indicative of the user identity or authorization and the system, file, or application with which the password is to be used. Of course, more complex associations are also possible when desired.

[0041] Referring now to Fig. 8, a flow diagram of a method of securely supporting password change for use with the method of Figure 7 wherein a choice is given to the user is shown. During the password change operation of step 80 and after user authorization at step 82 due to the detection of the password change operation at step 81, the user is given the opportunity to either enter a password or to have the process automatically generate a new password at step 83. Therefore, in the case of a computer-generated password, the user does not have to invent and remember the new password because it is automatically assigned to his authorization data and automatically retrieved for access to the system. Consequently, choosing a computer-generated password means that the new password is never typed in which decreases the possibilities of a Trojan Horse application from detecting same.

[0042] Advantageously, when a password is automatically generated, it is unknown to the user. This makes the password impossible to ascertain except by breaching security of password database. For example, when automatic password generation is used, an encryption key may form each password allowing for security relating to access and for encryption of file data to prevent mining of file data.

[0043] Numerous other embodiments may be envisaged without departing from the spirit and scope of the invention.

Claims

What is claimed is:

1. A method of securely supporting password change comprising the steps of:

detecting at least one of the operations in execution on a system comprising:

(i) detecting a password change operation (55; 62; 71; 81),

(ii) and detecting a new password storage operation (57);

performing an operation to change the password of a user to a new password in the system (53, 64, 74);

storing the new password in a password database on the system (54; 67; 76); and,

storing data indicative (59, 66; 75) of a new password for later retrieval of the new password by the system in a database independent of the change password operation and of the database where the new password is stored.

2. A method of securely supporting password change according to claim 1 wherein the step of detecting a password change operation (55; 62; 71; 81) in execution on a system comprises the step of detecting a new password prompt.

3. A method of securely supporting password change according to claim 1 comprising the steps of:

prompting a user to provide authorization data (72); and,

associating the authorization data with the password.

4. A method of securely supporting password change according to claim 1, wherein the step of detecting the new password comprises the step of detecting the new password at least two separate times.

5. A method of securely supporting password change according to claim1 wherein the operation detected is a password change operation and further comprising the steps of:

displaying to a user a prompt for a new password (63), the prompt independent of the password change operation;

IPR2022-00412
Apple EX1053 Page 767

receiving the new password (65);

6. A method of securely supporting password change according to claim 5 wherein the step of detecting the change password operation in execution on a system comprises the step of detecting password change command options.

7. A method of securely supporting password change according to claim 1 wherein the operation detected is a password change operation and further comprising the steps of:

displaying to a user a prompt for authentication information (72), the prompt independent of the password change operation;

receiving the authentication information (73);

when the authentication information is indicative of a known user, performing said operation to change the password (74) of the known user to a new password in the system; and;

8. A method of securely supporting password change according to claim 7 wherein the prompt for authentication information is a prompt for biometric information.

9. A method of securely supporting password change according to claim 8 comprising the step of:

providing biometric information;

processing the provided biometric information to provide biometric data;

comparing the biometric data with a stored template; and

in dependence upon a comparison result retrieving a user password from a database.

10. A method of securely supporting password change according to claim 7 wherein the prompt for authentication information is a prompt for information stored on a smart card.

11. A method of securely supporting password change according to claim 7 wherein the step of performing an operation to change the password comprises the step of providing the new password to the system.

12. A method of securely supporting password change according to claim 7 wherein the step of performing an operation to change the password comprises the step of prompting the user to select between provision of the new password and automatic generation of the new password (83).

13. A method of securely supporting password change according to any of claims 7 and 12, characterized in that the step of performing an operation to change the password comprises the step of automatically generating the new password.

14. A method of securely supporting password change according to claim 13 wherein data secured with the new password is encrypted using an encryption key.

15. A method of securely supporting password change according to claim 7 comprising the step of performing another operation to change another password of the known user to the new password.

16. A method of securely supporting password change according to claim 7 comprising the step of determining all passwords identical to the password being changed and automatically performing at least another operation to change each identical password of the known user to the new password.

17. A method of securely supporting password change according to claim 1 wherein the operation detected is a password change operation;
wherein the system has a known user authorized thereon; and,
wherein the step of performing an operation to change the password comprises the step of automatically generating a new password .

18. A method of securely supporting password change according to any of claims 13 and 17, characterized in that the automatically generated new password is unknown to the user.

19. A method of securely supporting password change according to any of claims 13 and 18, characterized in that the automatically generated new password is an encryption key.

20. A method of securely supporting password change according to any of claims 13 and 19, characterized in that the data secured with the new password is encrypted using an encryption key.

IPR2022-00412
Apple EX1053 Page 770

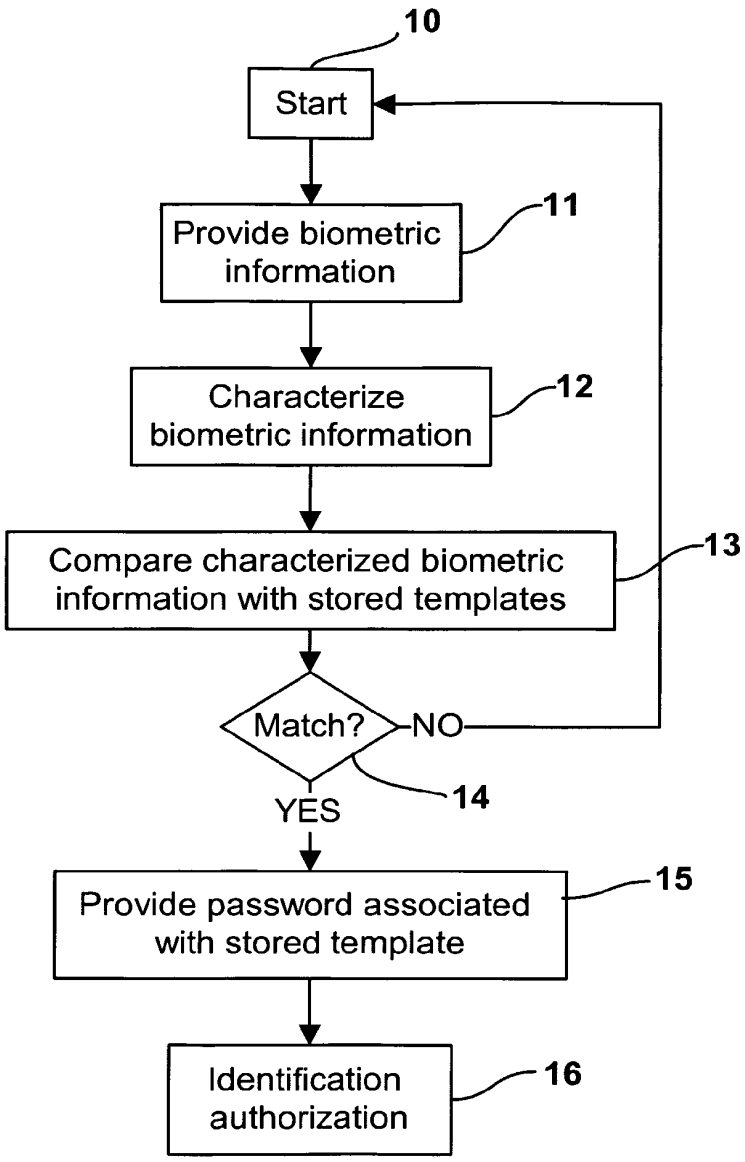


Fig. 1
(PRIOR ART)

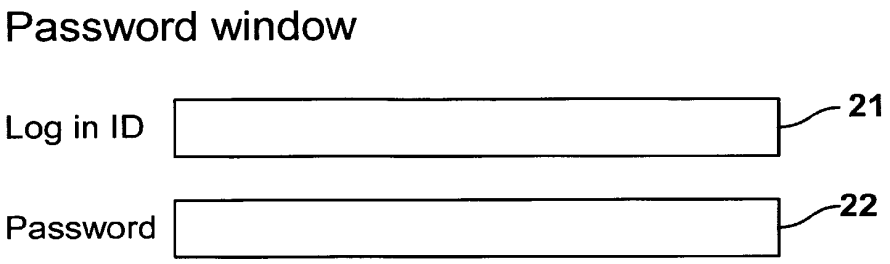


Fig. 2
(PRIOR ART)

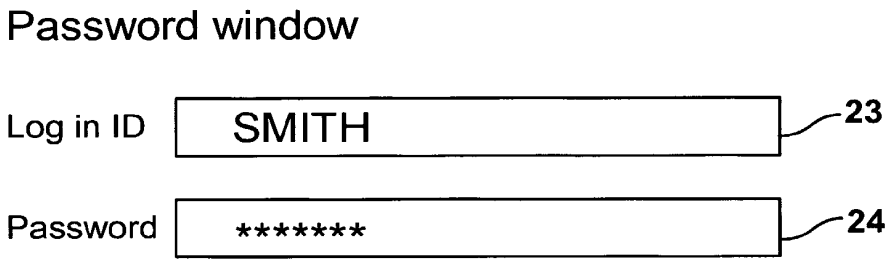


Fig. 2a
(PRIOR ART)

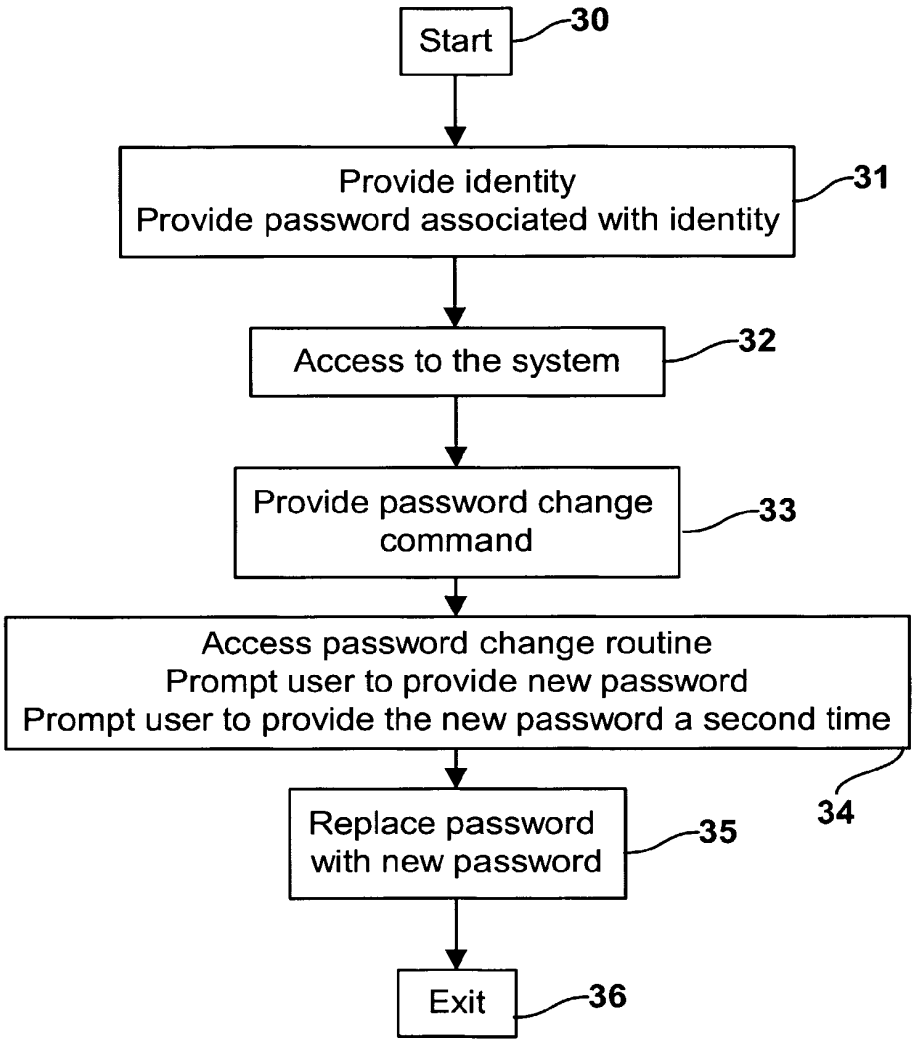


Fig. 3
(PRIOR ART)

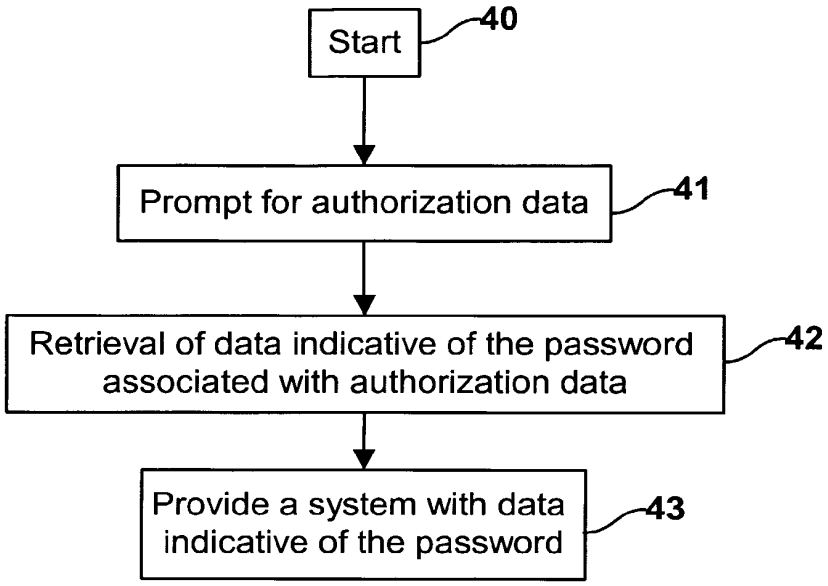


Fig. 4
(PRIOR ART)

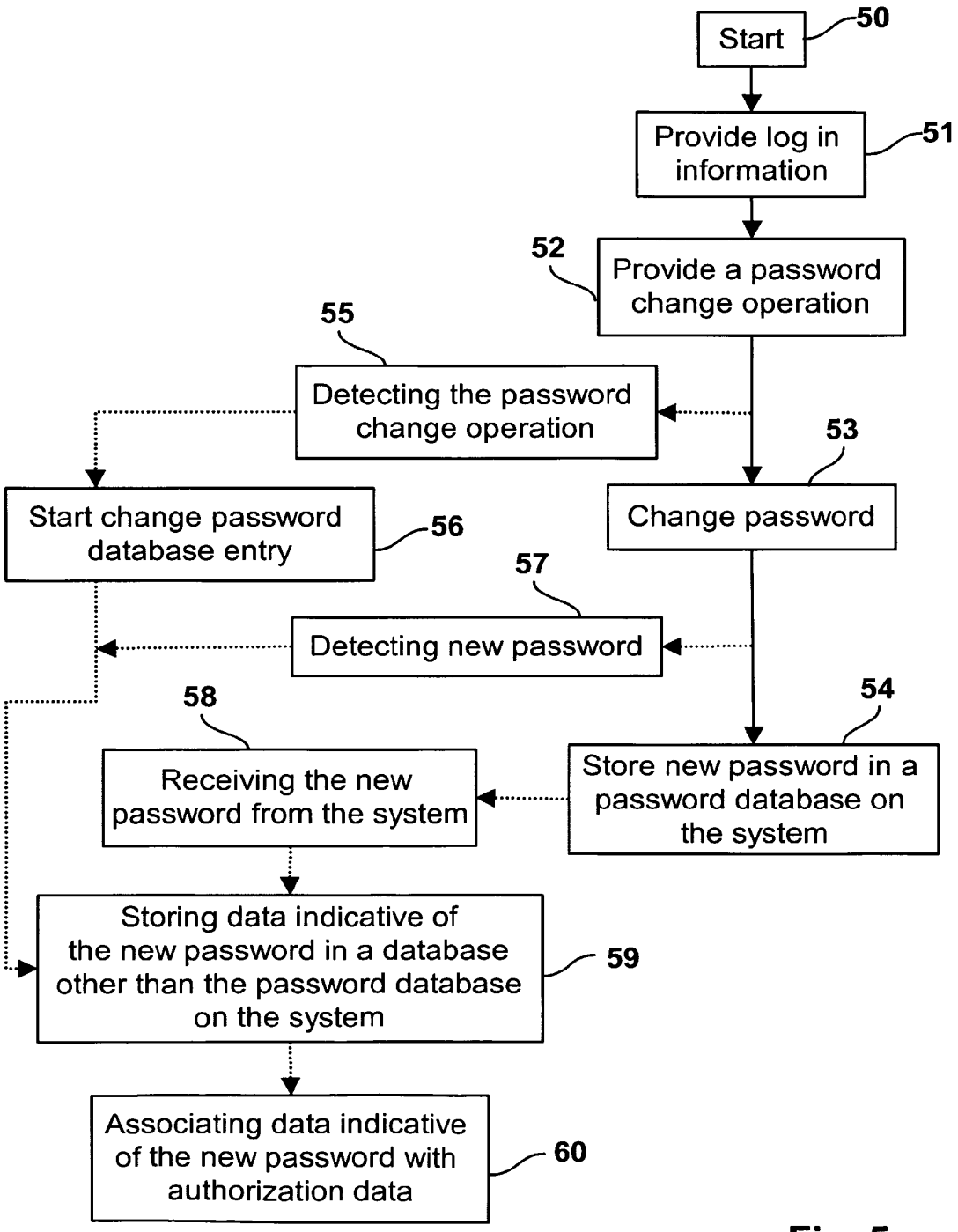

Start
50
Provide log in information
51
52
Provide a password change operation
55
Detecting the password change operation
53
Start change password database entry
56
Change password
57
Detecting new password
58
54
Receiving the new password from the system
Store new password in a password database on the system
Storing data indicative of the new password in a database other than the password database on the system
59
Associating data indicative of the new password with authorization data
60

Fig. 5

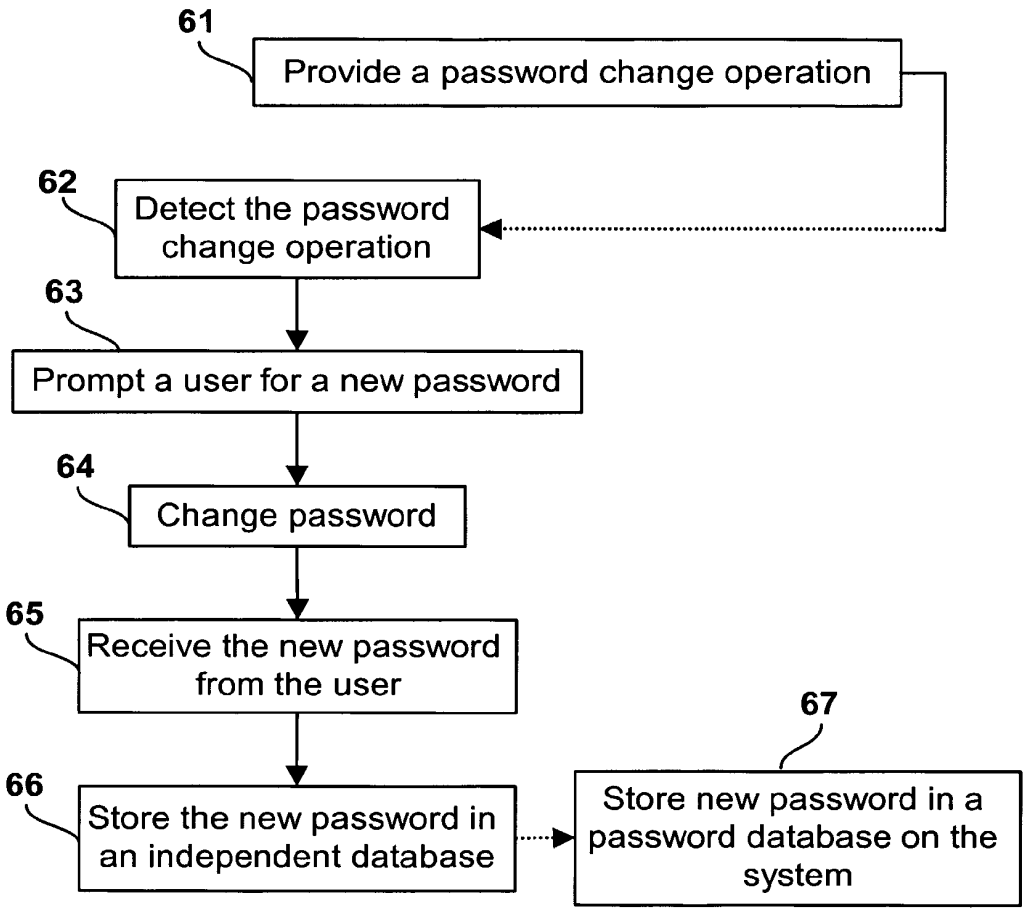

61
Provide a password change operation
62
Detect the password change operation
63
Prompt a user for a new password
64
Change password
65
Receive the new password from the user
66
Store the new password in an independent database
67
Store new password in a password database on the system

Fig. 6

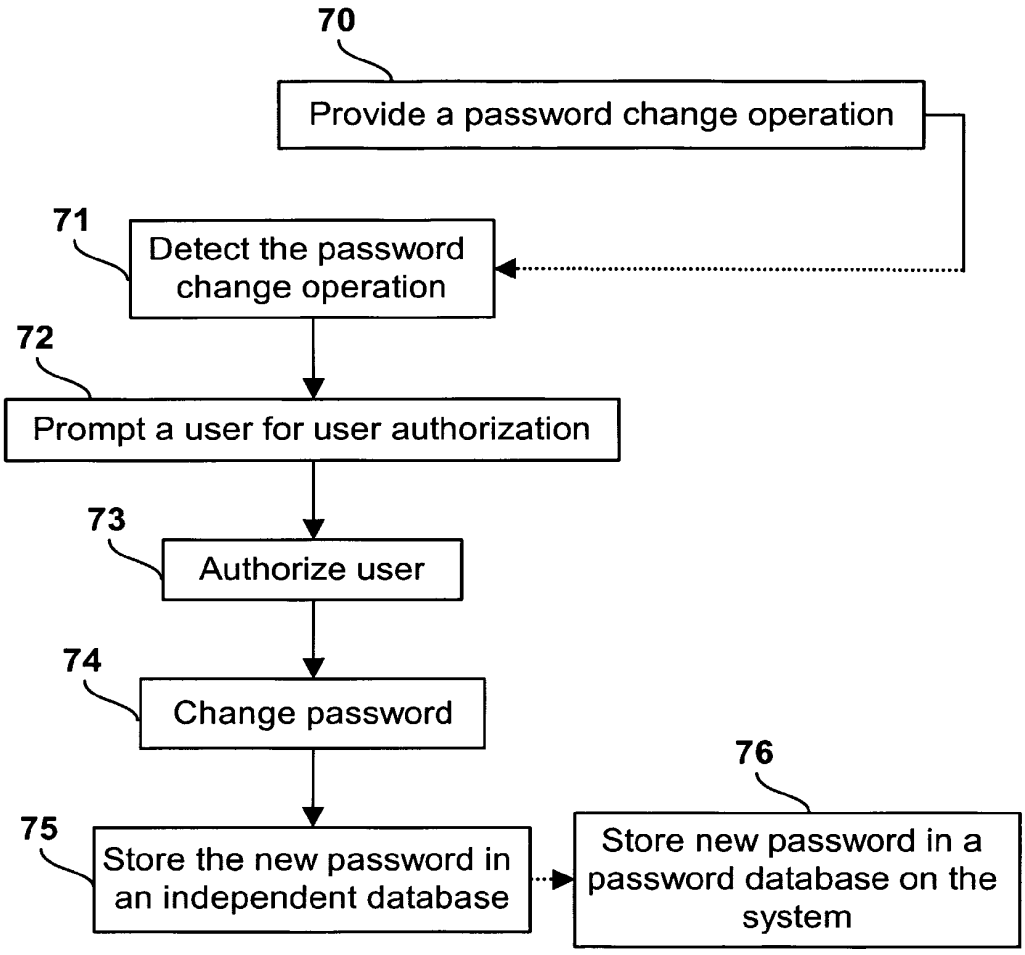

70
Provide a password change operation
71
Detect the password change operation
72
Prompt a user for user authorization
73
Authorize user
74
Change password
75
Store the new password in an independent database
76
Store new password in a password database on the system

Fig. 7

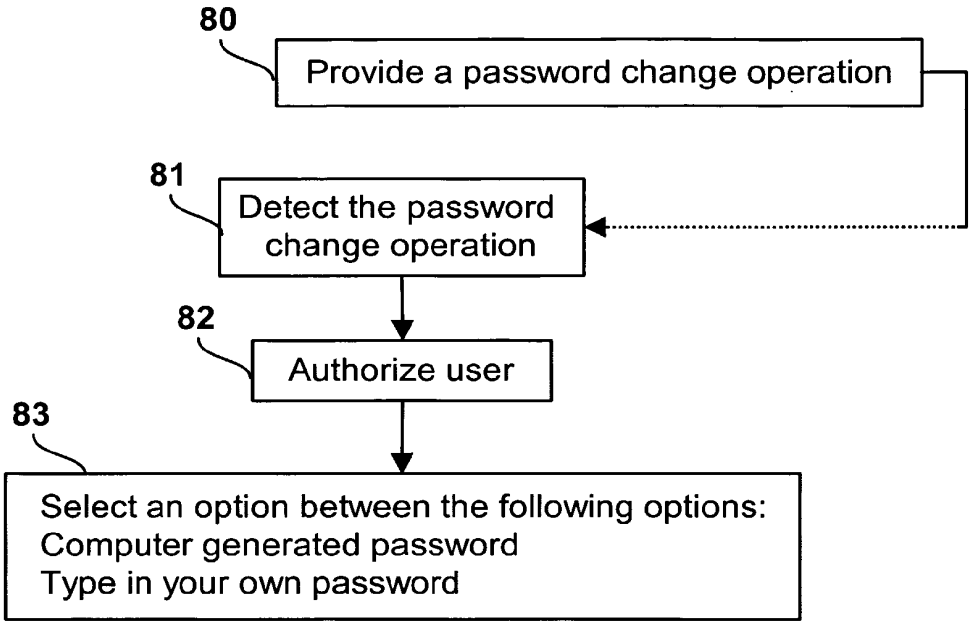

80
Provide a password change operation
81
Detect the password change operation
82
Authorize user
83
Select an option between the following options:
Computer generated password
Type in your own password

Fig. 8

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
31 décembre 2003 (31.12.2003)

PCT

(10) Numéro de publication internationale
WO 2004/002058 A2

(51) Classification internationale des brevets[7] : H04L 9/30

(21) Numéro de la demande internationale :
PCT/FR2003/001871

(22) Date de dépôt international : 18 juin 2003 (18.06.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/07688 19 juin 2002 (19.06.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMPLUS** [FR/FR]; Parc d'Activités de Gémenos, Avenue du Pic-de-Bertagne, F-13420 Gémenos (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **FEYT, Nathalie** [FR/FR]; 8, chemin de Raphèle, 7 lotissement l'Oliveraie, F-13780 Cuges les Pins (FR). **JOYE, Marc** [FR/FR]; 19, rue Voltaire, F-83640 Saint Zacharie (FR).

(74) Mandataire : **AIVAZIAN, Denis**; Gemplus la Vigie, Service brevets, BP 100, F-13705 La Ciotat Cedex (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— *relative à l'identité de l'inventeur (règle 4.17.i)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *relative au droit du déposant de demander et d'obtenir un brevet (règle 4.17.ii)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

[Suite sur la page suivante]

(54) **Title:** METHOD OF GENERATING ELECTRONIC KEYS FOR A PUBLIC-KEY CRYPTOGRAPHY METHOD AND A SECURE PORTABLE OBJECT USING SAID METHOD

(54) **Titre :** PROCEDE DE GENERATION DE CLES ELECTRONIQUES POUR PROCEDE DE CRYPTOGRAPHIE A CLE PUBLIQUE ET OBJET PORTATIF SECURISE METTANT EN OEUVRE LE PROCEDE

(57) **Abstract:** The invention relates to a method of generating electronic keys (d) for a public-key cryptography method using an electronic device. The inventive method comprises two separate calculation steps, namely: step A consisting in (i) calculating pairs of prime numbers (p, q), said calculation being independent of knowledge of the pair (e, l) in which e is the public exponent and l is the length of the key of the cryptography method, and (ii) storing the pairs thus obtained; and step B which is very quick and can be executed in real time by the device, consisting in calculating a key d from the results of step A and knowledge of the pair (e, l).

(57) **Abrégé :** L'invention concerne un procédé de génération de clés électroniques d pour procédé de cryptographie à clé publique au moyen d'un dispositif électronique. Selon l'invention, le procédé comprend deux étapes de calcul dissociées. Une étape A consiste à - calculer des couples de nombres premiers (p, q), ce calcul est indépendant de la connaissance du couple (e, l) e l'exposant public et l la longueur de la clé du procédé de cryptographie et à - stocker les couples ainsi obtenus. Une étape B très rapide qui peut être exécutée en temps réel par le dispositif, consiste à calculer une clé d à partir des résultats de l'étape A et de la connaissance du couple (e, l).

WO 2004/002058 A2

IPR2022-00412
Apple EX1053 Page 779

— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour toutes les désignations*
— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :
— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

PROCEDE DE GENERATION DE CLES ELECTRONIQUES POUR PROCEDE DE CRYPTOGRAPHIE A CLE PUBLIQUE ET OBJET PORTATIF SECURISE METTANT EN ŒUVRE LE PROCEDE

L'invention concerne un procédé de génération de clés électroniques pour procédé de cryptographie à clé publique. Elle concerne également un objet portatif sécurisé mettant en œuvre le procédé.

L'invention concerne plus particulièrement la génération de clés d'un système cryptographique de type RSA et leur stockage sur un objet sécurisé en vue de leur utilisation dans une application nécessitant de la sécurité.

L'invention s'applique tout particulièrement à dés objets sécurisés ne possédant pas d'importante ressource mémoire telle que de la mémoire électriquement programmable, ni de ressources de calcul puissantes comme c'est le cas pour les cartes à puce.

Une application de l'invention est le commerce électronique par l'intermédiaire d'un téléphone portable. Dans ce contexte les clés peuvent se trouver sur la carte SIM du téléphone.

Il est en effet prévu que certains programmes d'applications utilisent de telles clés pour mettre en œuvre un transfert de données confidentielles, dans un contexte de commerce électronique par exemple. Par la suite, on considèrera que ces applications sont fournies par une entité fournisseur de service.

En outre, il est connu que pour garantir l'intégrité de la clé, on lui associe généralement un certificat fourni par une entité de confiance.

IPR2022-00412
Apple EX1053 Page 781

Parmi les procédés de cryptographie à clé publique, on s'intéresse dans ce qui suit au protocole de cryptographie RSA (Rivest Shamir et Adleman). Ce protocole met en œuvre une étape de génération de nombres premiers de grande taille, coûteuse en temps de calcul et en place mémoire.

On rappelle que ce protocole de cryptographie RSA permet le chiffrement d'informations et/ou l'authentification entre deux entités et/ou la signature électronique de messages.

Le protocole de cryptographie RSA est le plus utilisé car il possède des propriétés qui lui permettent d'être employé aussi bien en chiffrement qu'en génération de signature.

Pour ce faire, le système de cryptographie RSA comprend un algorithme « public » réalisant la fonction de chiffrement ou de vérification de signature et un algorithme « privé » réalisant la fonction de déchiffrement ou de génération de signature.

Sa sécurité repose sur la difficulté de factorisation d'un nombre entier public N de grande taille qui est le produit de deux nombres premiers secrets p et q de grande taille, le couple (p,q) entrant dans le calcul de la clé secrète d utilisée par la fonction de déchiffrement ou par la fonction de calcul d'une signature.

Afin de mieux comprendre le problème qui va être exposé dans la suite, on va rappeler dans ce qui suit les paramètres entrant dans un schéma de cryptographie RSA :.

1) L'exposant public e :

IPR2022-00412
Apple EX1053 Page 782

Il est propre à une application et est fourni par cette application. De ce fait, il est commun à tous les utilisateurs de cette même application.

2) Les paramètres p et q:

Ils sont générés à l'issu d'un calcul coûteux en temps. Ils ont en général la même longueur (même taille). Cette longueur est classiquement de 512 bits. Pour augmenter la sécurité, cette longueur peut aller de 512 bits à 2048, 2048 bits étant envisagés pour le futur.

3) N est le module public et est calculé à partir de la relation suivante :

$N = p*q$

La clé de l'algorithme est dite de longueur ℓ, lorsque le module public N est de longueur ℓ. Cette longueur est fixée par l'application (ou fournisseur de service).

4) les paramètres e et N forment la clé publique.

5) la clé privée d est calculée à partir de la relation suivante :

$d = 1/e[\text{mod}(p-1)(q-1)]$; $(1/e = e^{-1})$

soit encore $ed \equiv 1$ [(mod ppcm(p-1, q-1)] ; ppcm signifie le plus petit commun multiple,

les paramètres secrets sont formés par le triplet (d, p, q).

6) la forme « normale » de la clé privée est:

(d,N).

6) la forme CRT (Chinese Remainder Theorem) de la clé privée est:

dans ce cas la clé privée comporte 5 paramètres :

p, q

d_p avec $d_p = d \text{ mod}(p-1)$

d_q avec $d_q = d \text{ mod}(q-1)$

I_q avec $I_q = q^{-1} \text{ mod}p$.

IPR2022-00412
Apple EX1053 Page 783

Le principe de la génération d'une clé selon le, schéma RSA consiste donc comme on peut le voir, à générer une clé privée d à partir d'un exposant public e (ou clé publique) fixé par l'application, les paramètres p, q étant générés de sorte que p*q = N, la longueur ℓ de N étant fixée.

Lorsque plusieurs applications sont prévues, chaque fournisseur de service fournit son exposant public e et la longueur du module public N, de manière à ce que puisse être générée la clé privée d correspondante.

Ainsi, la mise en œuvre d'un calcul de clé RSA nécessite la connaissance de l'exposant public e et celle de la longueur ℓ de la clé de l'algorithme c'est à dire la longueur du modulo N. Avec les données d'entrée e et ℓ, il reste à générer le couple de nombre premier p et q de manière à ce que ces derniers répondent aux conditions suivantes :

(i) p-1 et q-1 premiers avec e et,

(ii) N= p*q un nombre entier de longueur ℓ.

Ces contraintes sont coûteuses en temps de calcul.

On rappelle à ce propos que la génération et le stockage des clés pour des objets portables tels que les cartes à puce s'effectuent à ce jour des deux manières suivantes :

Selon une première manière, le calcul d'une clé RSA est effectué sur un serveur pour profiter d'une puissance de calcul importante. On requiert alors pour plus de sécurité, un certificat que l'on télécharge avec la clé au sein de l'objet sécurisé lors de sa phase de personnalisation.

Cette solution présente deux inconvénients. :

IPR2022-00412
Apple EX1053 Page 784

- d'une part malgré le cadre relativement sécurisé de la personnalisation, il peut y avoir vol ou duplication de la clé du fait de son transfert du serveur vers l'objet sécurisé, et

- d'autre part, chaque clé est chargée dans l'objet dans une phase initiale de personnalisation, ce qui nécessite de prévoir un maximum de clés dans chaque objet pour pouvoir anticiper les futurs besoins.

Dans la pratique, on stocke dans l'objet portable des ensembles de clés et de certificats correspondant à chaque application susceptible d'être utilisée, sans savoir si ces clés seront réellement utiles ultérieurement. Un emplacement mémoire important est utilisé inutilement. Par exemple 0,3 Koctets sont nécessaires pour une clé de RSA de module de 1024bits, alors que les cartes actuelles ont au plus 32Koctets de mémoire programmable. En outre, un nombre important de certificats est acheté à l'entité de confiance ce qui est coûteux.

L'inconvénient ultime mais tout aussi important est qu'il n'est pas possible d'ajouter de nouvelles clés au fur et à mesure que de nouvelles applications pourraient être envisagées.

Selon une deuxième solution, le calcul peut être effectué au sein de l'objet sécurisé. Cela résout le premier inconvénient de la solution précédente mais crée une lourdeur de traitement au niveau de l'objet sécurisé qui possède une faible capacité de calcul.

En effet, lorsque la génération d'une clé RSA est réalisée par un objet portatif tel qu'une carte à puce, si la longueur imposée de clé RSA est de 2048 bits, le calcul prend alors 30 secondes avec un algorithme performant.

IPR2022-00412
Apple EX1053 Page 785

Même si ce temps de calcul est acceptable pour certaines applications car on génère les clés RSA une seule fois pour une application donnée, ceci n'est pas satisfaisant pour les services de téléphonie mobile (GSM par exemple) car cette opération se renouvelle à chaque changement de carte SIM et qu'un plus grand nombre de clés doit être prévu pour répondre aux besoins de différentes applications.

Du fait d'un besoin en ressources de calcul important, les clés sont toujours crées durant la phase de personnalisation à partir des exposants publics e fournis par les différentes entités fournisseur de service. Cette étape de calcul ne peut pas être mise en œuvre ultérieurement car elle paralyserait le fonctionnement de l'objet.

De façon pratique ce calcul n'est pas mis en œuvre par la carte. En effet, ce calcul est long et il pourrait ralentir la phase de personnalisation, de plus sa durée est variable et elle pourrait se révéler incompatible avec les procédés de personnalisation des cartes à puce.

D'autre part, cette solution présente toujours le second inconvénient de la solution précédente à savoir la nécessité de ressource mémoire.

La présente invention a pour but de résoudre ces problèmes.

Plus précisément l'invention a pour objectif de résoudre le problème de lourdeur du calcul lié à la gestion de génération de clés ainsi que le problème de manque de flexibilité dû au stockage initial et définitif d'un nombre important de clés et de certificats en phase de personnalisation.

IPR2022-00412
Apple EX1053 Page 786

A cette fin, un objet de la présente invention concerne un procédé de génération de clés électroniques d pour procédé de cryptographie à clé publique au moyen d'un dispositif électronique, principalement caractérisé en ce qu'il comprend deux étapes de calcul dissociées :

Etape A

1) Calcul de couples de nombres premiers (p,q) ou de valeurs représentatives de couples de nombres premiers, ce calcul étant indépendant de la connaissance du couple (e,l) dans lequel e est l'exposant public et l la longueur de la clé du procédé de cryptographie, l étant également la longueur du module N dudit procédé,
2) Stockage des couples ou des valeurs ainsi obtenus ;

Etape B

Calcul de la clé d à partir des résultats de l'étape A et de la connaissance du couple (e,l).

Selon une première variante, l'étape A-1) consiste à calculer des couples de nombres premiers (p,q) sans connaissance de l'exposant public e ni de la longueur l de la clé, en utilisant un paramètre Π qui est le produit de petits nombres premiers. De cette manière couple (p,q) obtenu à l'étape A, a une probabilité maximale de pouvoir correspondre à un futur couple (e,l) et permettra de calculer une clé d lors de la mise en œuvre de l'étape B.

Selon une autre variante dépendante de la variante précédente, le calcul A-1) tient compte en plus du fait que e a une forte probabilité de faire partie de l'ensemble $\{3, 17, \ldots, 2^{16+1}\}$, on utilise pour cela dans le

IPR2022-00412
Apple EX1053 Page 787

calcul de l'étape A, une graine σ qui permet de calculer non pas des couples (p,q) mais une valeur représentative appelée image des couples (p,q).

Le stockage A-2) consiste alors à mémoriser cette image. Ceci permet de gagner de la place mémoire puisqu'une image est plus petite qu'un nombre premier p ou q par exemple 32 octets comparés à 128 octets.

Selon une troisième variante on effectue un calcul de couples (p,q) pour différents couples (e,l) probables. De façon pratique le paramètre Π va contenir les valeurs usuelles de e par exemple 3, 17.

Selon une quatrième variante l'étape A-1) comprend une opération de compression des couples (p,q) calculés et l'étape A-2) consiste alors à stocker les valeurs compressées ainsi obtenues.

L'étape B comprend la vérification des conditions suivantes pour un couple (e, ℓ) donné:

(i) p-1 et q-1 premiers avec e et,

(ii) N= p*q un nombre entier de longueur ℓ.

Selon un mode de réalisation préféré, l'étape A-1) comprend la génération d'un nombre premier q, le choix d'une limite inférieure B_0 pour la longueur ℓ_0 de ce nombre premier à générer telle que $\ell_0 \geq B_0$ par exemple B_0= 256 bits, et elle comprend en outre les sous-étapes suivantes :

1) -calculer des paramètres v et w à partir des relations suivantes et les mémoriser:

$$v = \sqrt{2^{2\ell_0 - 1}} / \Pi$$

$$w = 2^{\ell_0} / \Pi$$

dans lesquelles Π est mémorisé et correspond au produit des f plus petits nombres premiers, f étant choisi de manière telle que $\Pi \leq 2^{B_0}$,

IPR2022-00412
Apple EX1053 Page 788

2)-choisir un nombre j dans l'intervalle des nombres entiers {v,….,w-1} et calculer $\ell = j\ \Pi$;

3)-choisir et enregistrer un nombre premier k de longueur courte par rapport à la longueur d'une clé RSA dans l'intervalle des nombres entiers {0,…., $\Pi-1$} , (k, Π) étant co-premiers, ;

4)-calculer $q = k+\ell$,

5)-vérifier que q est un nombre premier, si q n'est pas un nombre premier alors :

a) prendre une nouvelle valeur pour k au moyen de la relation suivante :

$k = a\,k\ (mod\ \Pi)$; a appartenant au groupe multiplicatif Z^*_Π des nombres entiers modulo Π;

b) réitérer à partir de la sous-étape 4).

Avantageusement l'étape B comprend, pour un couple (p,q) obtenu à l'étape A,et un couple (e,l) donné :

- La vérification des conditions suivantes :
  - (i) p-1 et q-1 premiers avec e et,
  - (ii) N= p*q un nombre entier de longueur ℓ,
- Si le couple (p,q) ne répond pas à ces conditions :
- Choix d'un autre couple et réitération de la vérification jusqu'à ce qu'un couple convienne,
- Calcul de la clé d à partir du couple (p,q) obtenu à l'issue de cette vérification.

L'invention a également pour objet, un objet sécurisé portatif apte à générer des clés électroniques d d'un algorithme de cryptographie de type RSA, caractérisé en ce qu'il comprend au moins :

- Des moyens de communication pour recevoir au moins un couple (e,l),

IPR2022-00412
Apple EX1053 Page 789

- Une mémoire pour stoker les résultats d'une étape A consistant à :

Calculer des couples de nombres premiers (p,q) ou de valeurs représentatives de couples de nombres premiers, ce calcul étant indépendant de la connaissance du couple (e,l) dans lequel e est l'exposant public et l la longueur de la clé du procédé de cryptographie, l étant également la longueur du module N dudit procédé,

- Un programme pour mettre en œuvre une étape B consistant à :

Calculer d'une clé d à partir des résultats de l'étape A et de la connaissance d'un couple (e,l),

L'objet sécurisé portatif comprend en outre un programme pour la mise en œuvre de l'étape A, les étapes A et B étant dissociées dans le temps.

L'objet sécurisé portatif pourra être constitué par une carte à puce.

D'autres particularités et avantages de l'invention apparaîtront clairement à la lecture de la description qui est donnée ci-après à titre d'exemple non limitatif et en regard de la figure unique représentant un schéma d'un système de mise en œuvre du procédé.

La suite de la description est faite dans le cadre de l'application de l'invention à un objet portatif de type carte à puce et pour simplifier l'expression on parlera de carte à puce.

Selon le procédé proposé la génération de clés se fait en deux étapes dissociées.

IPR2022-00412
Apple EX1053 Page 790

La première Etape A comporte un calcul de couples de nombres premiers (p,q) ou de valeurs représentatives de couples de nombres premiers appelée image.

Les couples (p,q) obtenus sont stockés.

Ce calcul est lourd et il est d'autant plus lourd si on utilise un algorithme de génération de nombres premiers classique.

Il est proposé ici que ce calcul soit effectué de manière indépendante de la connaissance du couple (e,l).

Comme cela va être détaillé dans la suite un mode de réalisation préféré pour mettre en œuvre cette étape permet d'alléger les calculs et de limiter la place mémoire nécessaire pour le stockage des couples (p,q) obtenus en stockant une image de ces couples.

La deuxième Etape B comporte le calcul à proprement parler de la clé d à partir des résultats de l'étape A et de la connaissance du couple (e,l).

Ce calcul comprend, pour un couple (p,q) obtenu à l'étape A, et un couple (e,l) donné :

- La vérification des conditions suivantes :
  (i) p-1 et q-1 premiers avec e et,
  (ii) N= p*q , ce nombre doit être un nombre entier et de longueur ℓ,
- Si un couple (p,q) ne répond pas à ces conditions, on choisit un autre couple et on réitère de la vérification jusqu'à ce qu'un couple convienne parmi les couples obtenus lors de l'étape A.
- On peut procéder alors au calcul de la clé d à partir du couple (p,q) obtenu à l'issue de cette vérification.

La première étape qui correspond à un calcul relativement lourd par rapport à la deuxième étape, peut être exécutée par un autre organe que la carte à

IPR2022-00412
Apple EX1053 Page 791

puce par exemple par un serveur. Dans ce cas, les résultats du calcul de cette première étape pourront être chargés sur une carte à puce au moment de la personnalisation.

Le calcul de l'étape A peut également être fait par la carte elle-même à un instant quelconque qui ne gêne pas l'utilisateur de cette carte. Par exemple, ce calcul peut être fait lors de la personnalisation de la carte ou plus tard.

De façon pratique, lors de l'utilisation de la carte, pour obtenir un service, si une clé privée est nécessaire, alors la clé publique est fournie par le fournisseur de service (éventuellement à distance si elle n'est pas déjà stockée dans la carte) afin de générer la clé privée. Cette étape de génération (étape B de calcul) est effectuée de manière rapide par la carte.

On voit donc que de nouvelles applications qui nécessitent le calcul d'une clé privée d peuvent être prévues pour une carte.

On voit également qu'il n'y a pas besoin d'associer un certificat aux couples (p,q) car ils ne sont pas associés à une clé privée.

Ainsi, la génération d'une clé privée peut être faite à bord c'est à dire par la carte elle-même avec un gain d'un facteur 10 en temps d'exécution par rapport aux procédés de génération de clés connus à ce jour.

On va décrire dans ce qui suit un mode préféré de réalisation pour la mise en œuvre de l'étape A. Ce mode de réalisation est particulièrement avantageux pour la mise à bord d'une carte à puce car il permet

IPR2022-00412
Apple EX1053 Page 792

d'optimiser à la fois la place mémoire mais aussi le temps de calcul.

Tout d'abord, afin de s'assurer que N=p*q est un entier de ℓ-bit, on choisit p appartenant à l'intervalle :

$$\left[\sqrt{2^{2(l-l0)-1}}, 2^{l-l0}-1\right]$$

Et q appartenant à l'intervalle :

$$\left[\sqrt{2^{2l0-1}}, 2^{l0}-1\right]$$

Pour ℓ_0 compris entre 1 et ℓ.

Ainsi min(p)min(q) est compris entre $2^{\ell 0}$-1 et N, et max(p)max(q) est compris entre N et 2^{ℓ} comme cela est demandé.

De cette façon, la condition ii) ci-dessus mentionnée se réduit à rechercher des nombres premiers dans l'intervalle :

$$\left[\sqrt{2^{2l0-1}}, 2^{l0}-1\right]$$

La solution proposée exploite le paramètre Π. Ce paramètre Π est le produit de petits nombres premiers dans lequel on peut trouver notamment 3, 17, 2^{16+1}, nombres premiers généralement utilisés comme exposants publics. Ainsi, la probabilité pour qu'un couple (p,q) corresponde à un futur couple (e,l) donné, déjà très élevée, augmente encore lorsque Π comporte de telles valeurs.

On choisit les f plus petits nombres premiers, f étant choisi de manière telle que $\Pi_i p_i \leq 2B_0$, B_0 est la

borne inférieure choisie pour ℓ_0. par exemple on peut choisir B_0 égal à 256 bits.

Π est égal au produit : 2.3…..191 et est inférieur à 2^{256}.

On peut alors mémoriser cette valeur Π dans la carte par exemple comme une constante dans la mémoire morte de programme.

La première phase du procédé consiste à générer et à enregistrer un nombre premier k de longueur courte par rapport à la longueur d'une clé RSA dans l'intervalle des nombre entiers $\{0,\ldots., \Pi-1\}$, (k, Π) étant copremiers, c'est à dire n'ayant pas de facteur commun.

La deuxième phase consiste ensuite à partir de ce nombre k à construire le premier candidat q qui satisfait la condition d'être copremier avec Π .

Si ce premier candidat ne satisfait pas cette condition, alors il est mis à jour c'est à dire qu'un autre candidat est choisi jusqu'à ce qu'une valeur de q satisfaisant à la condition soit trouvée.

On va présenter dans la suite les différentes étapes de l'algorithme de génération d'un nombre premier entrant dans le calcul d'une clé RSA selon l'invention.

L'algorithme proposé fonctionne quelle que soit la longueur lo donnée pour le nombre premier q qui doit être généré.

La génération du nombre premier p est identique, il suffit de remplacer q par p dans les étapes qui vont être développées et de remplacer lo par l-lo.

Après avoir fixé la limite Bo, on calcule les nombres premiers uniques v et w satisfaisant les conditions suivantes:

IPR2022-00412
Apple EX1053 Page 794

$$\sqrt{2}\,2^{\ell_0-1} \le v\Pi \le \sqrt{2}\,2^{\ell_0-1} + \Pi,$$
$$2^{\ell_0} - \Pi \le w\Pi \le 2^{\ell_0}$$

Ceci, se traduit par le calcul de v et w par les relations suivantes :

$$v = \sqrt{2}\,2^{2\ell_0-1} / \Pi$$
$$w = 2^{\ell_0} / \Pi$$

Puis après avoir pris k appartenant au groupe multiplicatif $Z^*\Pi$ des nombres entiers modulo Π, on construit le premier candidat q tel que,

$q = k + j\,\Pi$ pour tout j appartenant à l'intervalle [v, w-1] .

Comme justement k apparient à $Z^*\Pi$, la probabilité pour avoir un premier candidat q premier, est élevée. Si ce n'est pas le cas, on met à jour k en prenant k égal à ak(mod Π), a appartenant au groupe $Z^*\Pi$ et on réitère jusqu'à trouver une valeur de q correspondant à un nombre premier.

Une manière de tester la primalité d'un nombre est par exemple d'utiliser le test de Rabin-Miller.

Les différentes étapes de l'algorithme proposé sont précisément les suivantes :

1) -calculer des paramètres v et w à partir des relations suivantes et les mémoriser:

$$v = \sqrt{2}\,2^{2\ell_0-1} / \Pi$$
$$w = 2^{\ell_0} / \Pi$$

dans lesquelles Π est mémorisé et correspond au produit des f plus petits nombres premiers, f étant choisi de manière telle que $\Pi \le 2^{B_0}$,

2)-choisir un nombre j dans l'intervalle des nombres entiers {v,….,w-1} et calculer $\ell = j\,\Pi$;

3)-choisir et enregistrer un nombre premier k de longueur courte par rapport à la longueur d'une clé RSA dans l'intervalle des nombres entiers $\{0,\ldots., \Pi-1\}$, (k, Π) étant co-premiers, ;

4)-calculer $q= k+\ell$,

5)-vérifier que q est un nombre premier, si q n'est pas un nombre premier alors :

a) prendre une nouvelle valeur pour k au moyen de la relation suivante :

$k = a\,k \pmod{\Pi}$; a appartenant au groupe multiplicatif Z^*_Π des nombres entiers modulo Π;

b) réitérer à partir de l'étape 4) ;

6) enregistrer a, k' j pour les utiliser afin de retrouver q et ensuite exploiter q pour l'utiliser lors d'un calcul ultérieur de génération d'une clé RSA.

Au lieu de stocker la valeur de q on va procéder avantageusement comme décrit dans la suite.

Une manière simple de mettre en œuvre cet algorithme peut consister pour chaque longueur de clé RSA envisagée, de stocker les valeurs de k et j de manière à re construire q.

Plutôt que de choisir un nombre aléatoire j comme indiqué à l'étape 2) un autre mode de réalisation peut consister à construire j à partir d'un nombre aléatoire court.

On prend par exemple un nombre de longueur 64-bit, que l'on désigne par graine et que l'on dénote σ. Cette graine est alors prise comme valeur d'entrée d'un générateur de nombres pseudo-aléatoires PRNG, lequel va permettre de générer j.

j est alors défini comme $PRNG_1(\sigma) \pmod{(w-v)+v}$.

Ce mode d'exécution permet de réduire considérablement les besoins en place mémoire car il n'y a à stocker que les valeurs de σ et de k en mémoire

IPR2022-00412
Apple EX1053 Page 796

EEPROM. La valeur de Π est en mémoire morte (dans le programme de calcul).

On peut encore réduire les besoins en place mémoire en constatant que : si $k_{(o)}$ est la première valeur de k appartenant au groupe $Z^*\prod$, alors, les nombres premiers générés ont la forme :

$q = a^{f-1} k_{(o)} \bmod \Pi + j \Pi$

f étant le nombre d'échec du test de l'étape 4).

Cette valeur $k_{(o)}$ qui appartient au groupe $Z^*\prod$, peut être facilement calculée à partir d'une graine aléatoire courte comme σ par exemple et en utilisant la fonction de Carmichael de Π^2 dénotée $\lambda(\Pi)$.

En utilisant cette fonction on peut exprimer $k_{(o)}$ par la relation suivante :

$k_{(o)} = [PRNG_2(\sigma) + b^{PRNG3(\sigma)} (PRNG_2(\sigma)^{\lambda(\Pi)} - 1)] \pmod{\prod}$

b étant un élément d'ordre $\lambda(\Pi)$ appartenant à $Z^*\prod$.

Ces deux modes d'exécution permettent de réduire les besoins en place mémoire puisqu'on ne va devoir stoker dans ce cas, que la valeur de la graine σ et différentes valeurs de f pour les longueurs désirées de clés.

Pour des clés RSA de modulo supérieur à 2048 bits, les expériences numériques qui ont été faites par les inventeurs montrent que f est égal à 2^8. Ceci signifie que f peut être codé sur 1 byte soit 8 octets.

A titre d'exemple, pour générer des clés RSA de longueur allant de 512 à 2048 bits avec une granulité de 32 bits, il y a 49 longueurs de clé possibles. Il est donc nécessaire de stocker sur la carte un byte soit 8 octets correspondant à la valeur de σ. Il est également nécessaire de stocker les valeurs de f pour les nombres premiers p et q soit 2*49=98 octets. Ceci

IPR2022-00412
Apple EX1053 Page 797

fait au total 106 bytes soit 848 bits en mémoire EEPROM.

Un dernier mode d'exécution permettant de réduire la place mémoire, consiste à stoker dans le programme de calcul, c'est à dire en mémoire de programme, plusieurs valeurs de Π et les valeurs de $\lambda(\Pi)$ correspondantes pour différentes longueurs de clés envisagées. On peut remarquer qu'une grande valeur de Π conduit aux plus petites valeurs pour f.

Le nombre premier q généré selon l'étape 4) par l'algorithme qui vient d'être décrit satisfait comme on l'a vu précédemment à la condition :

$q= a^{f-1} k_{(o)} \bmod \Pi + j*\Pi$

Si e divise Π on peut exprimer q par la relation suivante :

$q= a^{f-1} k_{(o)} \bmod(e)$

Afin que la condition i) énoncée au début de la description soit remplie, il faut choisir a tel que $a=1 \pmod e$ et forcer $k_{(o)}$ de manière à ce qu'il soit différent de $1 \pmod e$.

Ainsi le nombre premier q obtenu satisfait la relation $q= k_{(o)}$ différent de $1 \pmod e$.

La génération du nombre premier p est identique, q est remplacé par p dans les étapes qui ont été développées et lo par l-lo.

Comme cela a été dit, le programme mettant en œuvre le procédé de la carte n'a pas besoin de connaître à priori l'exposant public e. Cet exposant peut donc être fourni à tout moment par une application chargée dans la carte.

IPR2022-00412
Apple EX1053 Page 798

Toutefois, on sait que pour la plupart des applications (plus de 95%), les valeurs de e utilisées sont les valeurs $\{3, 17, 2^{16}+1\}$.

Afin de couvrir le plus grand nombre d'applications, on va de façon préférentielle choisir a tel que $a= 1 \bmod(\{3, 17, 2^{16}+1\})$ et forcer $k_{(o)}$ différent de cette valeur : $1 \bmod(\{3, 17, 2^{16}+1\})$.

On choisit par exemple comme candidat possible pour a, le nombre premier $R= 2^{64}-2^{32}+1$ à condition que le plus grand commun diviseur de Π et de R soit égal à 1.

La condition requise pour $k_{(o)}$ peut être obtenue par le théorème du reste chinois.

Comme cela a été dit une autre alternative peut consister pour l'étape A-1) à calculer des couples de nombres premiers (p,q) pour différents couples (e,l) probables.

En conclusion, l'invention propose un procédé en deux étapes dissociées, la deuxième étape très rapide par rapport aux solutions connues, peut être exécutée en temps réel. Ce procédé est également peu coûteux en place mémoire.

En outre, il n'y a pas de limite pour de nouvelles applications non prévues à la personnalisation de la carte.

IPR2022-00412
Apple EX1053 Page 799

REVENDICATIONS

1. Procédé de génération de clés électroniques d pour procédé de cryptographie à clé publique au moyen d'un dispositif électronique, principalement caractérisé en ce qu'il comprend deux étapes de calcul dissociées :

Etape A

1) Calcul de couples de nombres premiers (p,q) ou de valeurs représentatives de couples de nombres premiers, ce calcul étant indépendant de la connaissance du couple (e,l) dans lequel e est l'exposant public et l la longueur de la clé du procédé de cryptographie, l étant également la longueur du module N dudit procédé,
2) Stockage des couples ou des valeurs ainsi obtenus ;

Etape B

Calcul d'une clé d à partir des résultats de l'étape A et de la connaissance du couple (e,l).

2. Procédé de génération de clés électroniques selon la revendication 1, caractérisé en ce que l'étape A-1) consiste à calculer des couples de nombres premiers (p,q) sans connaissance de l'exposant public e ni de la longueur l de la clé, en utilisant un paramètre Π qui est le produit de petits nombres premiers, de manière à ce que chaque couple (p,q) ait une probabilité maximale de pouvoir correspondre à un futur couple (e,l) et puisse permettre de calculer une clé d.

3. Procédé de génération de clés électroniques selon la revendication 2, caractérisé en ce que le

IPR2022-00412
Apple EX1053 Page 800

calcul de l'étape A-1) tient compte en plus du fait que e a une forte probabilité de faire partie de l'ensemble $\{3, 17, \ldots, 2^{16+1}\}$, on utilise pour cela dans ce calcul une graine σ qui permet de calculer non pas des couples (p,q) mais une valeur représentative appelée image des couples (p,q).

4. Procédé de génération de clés électroniques selon la revendication 1 et 3, caractérisé en ce le stockage A-2) consiste à mémoriser l'image des couples.

5. Procédé de génération de clés électroniques selon la revendication 1, caractérisé en ce que l'étape A-1) consiste à calculer des couples de nombres premiers (p,q) pour différents couples (e,l) probables.

6. Procédé de génération de clés électroniques selon les revendications 2 et 5, caractérisé en ce que le paramètre Π contient les valeurs usuelles de l'exposant public e par exemple 3, 17.

7. Procédé de génération de clés électroniques selon la revendications 1, caractérisé en ce que l'étape A-1) comprend une opération de compression des couples (p,q) calculés et l'étape A-2) consiste alors à stocker les valeurs compressées ainsi obtenues.

8. Procédé de génération de clés électroniques selon la revendication 1, caractérisé en ce que l'étape A-1) comprend la génération d'un nombre premier q, pour lequel on fixe une limite inférieure B_0 pour la longueur ℓ_0 de ce nombre premier à générer, telle que $\ell_0 \geq B_0$ par exemple B_0= 256 bits, et en ce qu'elle comprend les sous étapes suivantes :

IPR2022-00412
Apple EX1053 Page 801

1) -calculer des paramètres v et w à partir des relations suivantes et les mémoriser:

$v = \sqrt{2^{2\ell_0 - 1}} / \Pi$

$w = 2^{\ell_0} / \Pi$

dans lesquelles Π est mémorisé et correspond au produit des f plus petits nombres premiers, f étant choisi de manière telle que $\Pi \leq 2^{B_0}$,

2)-choisir un nombre j dans l'intervalle des nombres entiers $\{v,\ldots,w-1\}$ et calculer $\ell = j\ \Pi$;

3)-choisir et enregistrer un nombre premier k de longueur courte par rapport à la longueur d'une clé RSA dans l'intervalle des nombres entiers $\{0,\ldots,\ \Pi-1\}$, $(k,\ \Pi)$ étant co-premiers, ;

4)-calculer $q = k+\ell$,

5)-vérifier que q est un nombre premier, si q n'est pas un nombre premier alors :

a) prendre une nouvelle valeur pour k au moyen de la relation suivante :

$k = a\,k\ (\mathrm{mod}\,\Pi)$; a appartenant au groupe multiplicatif Z^*_Π des nombres entiers modulo Π;

b) réitérer à partir de l'étape 4) ;

9. Procédé de génération de clés électroniques selon les revendications 3 et 8, caractérisé en ce que les nombres j et k peuvent être générés à partir de la graine σ stockée en mémoire.

10. Procédé de génération de clés électroniques selon la revendication 8, caractérisé en ce que le nombre premier p est généré en réitérant toutes les sous étapes précédentes en remplaçant q par p et en remplaçant ℓ_0 par $\ell - \ell_0$.

IPR2022-00412
Apple EX1053 Page 802

11. Procédé de génération de clés électroniques selon l'une quelconque des revendications précédentes, caractérisé en ce que :

L'étape B comprend, pour un couple (p,q) obtenu à l'étape A, :

- La vérification des conditions suivantes :
  (i) p-1 et q-1 premiers avec e donné et,
  (ii) N= p*q un nombre entier de longueur ℓ donnée,
- Si le couple (p'q) ne répond pas à ces conditions :
- Choix d'un autre couple et réitération de la vérification jusqu'à ce qu'un couple convienne,
- Calcul de la clé d à partir du couple (p,q) obtenu.

12. Objet sécurisé portatif apte à générer des clés électroniques d d'un algorithme de cryptographie de type RSA, caractérisé en ce qu'il comprend au moins :

- Des moyens de communication pour recevoir au moins un couple (e,l),
- Une mémoire pour stoker les résultats d'une étape A consistant à :

  Calculer des couples de nombres premiers (p,q) ou de valeurs représentatives de couples de nombres premiers, ce calcul étant indépendant de la connaissance du couple (e,l) dans lequel e est l'exposant public et l la longueur de la clé du procédé de cryptographie, l étant également la longueur du module N de ce p,
- Un programme pour mettre en œuvre une étape B consistant à :

  Calculer une clé d à partir des résultats de l'étape A et de la connaissance d'un couple (e,l),

IPR2022-00412
Apple EX1053 Page 803

13. Objet sécurisé portatif selon la revendication 12, caractérisé en ce qu'il comprend en outre un programme pour la mise en œuvre de l'étape A, les étapes A et B étant dissociées dans le temps.

14. Objet sécurisé portatif selon la revendication 13, caractérisé en ce que le programme de mise en œuvre de l'étape A met en œuvre les sous-étapes :

1) -calculer des paramètres v et w à partir des relations suivantes et les mémoriser:

$$v = \sqrt{2^{2\ell_0 - 1}} / \Pi$$

$$w = 2^{\ell_0} / \Pi$$

dans lesquelles Π est mémorisé et correspond au produit des f plus petits nombres premiers, f étant choisi de manière telle que $\Pi \leq 2^{B_0}$, B_0 est une limite inférieure fixée pour la longueur ℓ_0 du nombre premier à générer telle que $\ell_0 \geq B_0$ par exemple B_0= 256 bits,

2)-choisir un nombre j dans l'intervalle des nombres entiers $\{v, \ldots, w-1\}$ et calculer $\ell = j\ \Pi$;

3)-choisir et enregistrer un nombre premier k de longueur courte par rapport à la longueur d'une clé RSA dans l'intervalle des nombres entiers $\{0, \ldots, \Pi - 1\}$, (k, Π) étant co-premiers, ;

4)-calculer $q = k + \ell$,

5)-vérifier que q est un nombre premier, si q n'est pas un nombre premier alors :

a) prendre une nouvelle valeur pour k au moyen de la relation suivante :

$k = a\,k \pmod{\Pi}$; a appartenant au groupe multiplicatif Z^*_Π des nombres entiers modulo Π;

b) réitérer à partir de l'étape 4).

IPR2022-00412
Apple EX1053 Page 804

15. Objet sécurisé portatif selon la revendication 12 ou 13 ou 14, caractérisé en ce qu'il est constitué par une carte à puce.

IPR2022-00412
Apple EX1053 Page 805

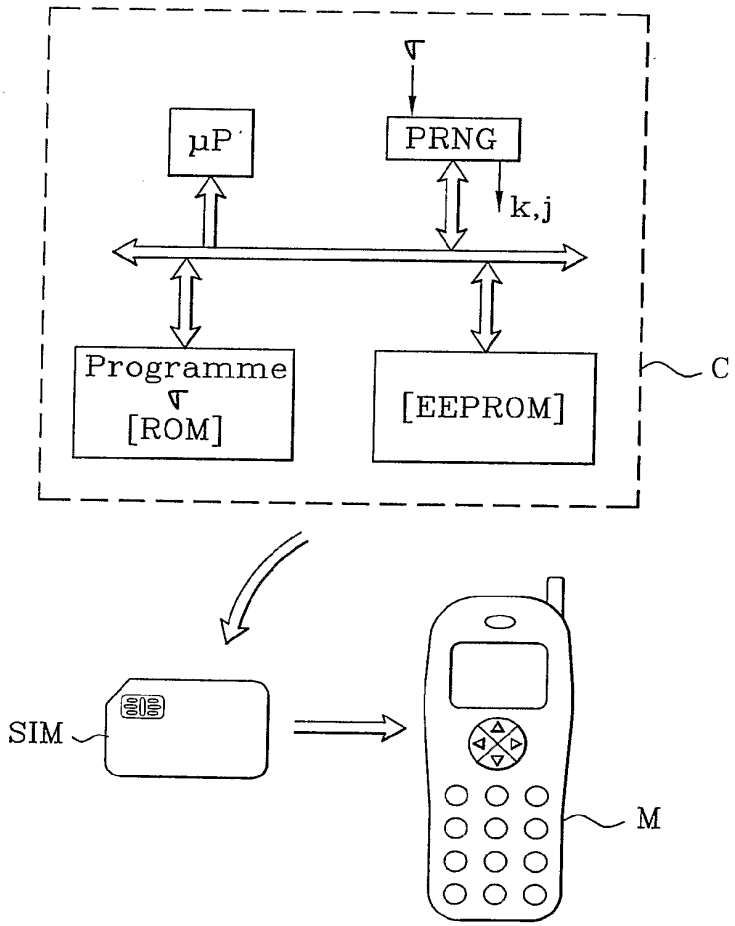


Figure unique

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 September 2004 (23.09.2004)

PCT

(10) International Publication Number
WO 2004/081706 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/SG2004/000024

(22) International Filing Date: 27 January 2004 (27.01.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2003901095 11 March 2003 (11.03.2003) AU

(71) Applicant *(for US only)*: **DIGISAFE PTE LTD** [SG/SG]; 100 Jurong East St 21, Singapore 609602 (SG).

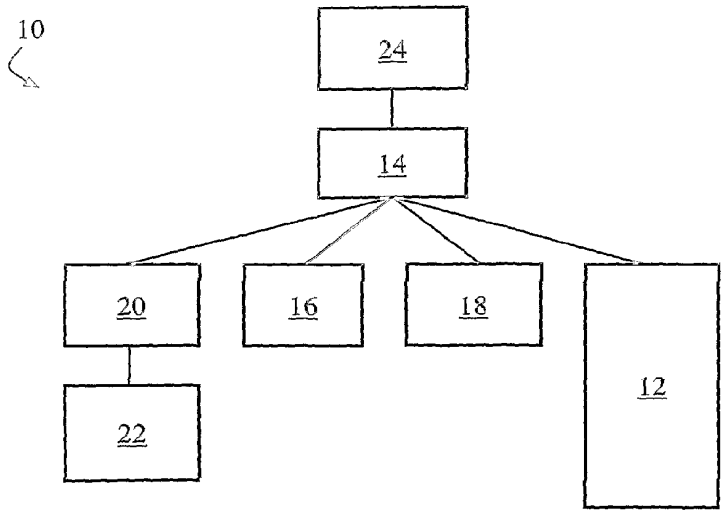
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **CHOW, Andrew** [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG). **LEE, Ser, Yen** [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG). **LAU, Puay, Hui** [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG). **CHIA, Boon, Quee** [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG). **TAN, Teck, Weng, Paul** [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG). **NG, Chee, We** [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG). **SOO, Hin, Meng, Timothy** [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG). **GATTAMENI, Venkateswara, Rao** [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG). **LOO, Whye, Ho, Jamez** [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG).

(74) Agent: **SIM, Yuan, Meng, Andrew**; Shook Lin & Bok, 1 Robinson Road, #18-00 AIA Tower, Singapore 048542 (SG).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD,

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR CONTROLLING THE PROVISION OF DIGITAL CONTENT



(57) Abstract: An apparatus for controlling the provision of digital content, comprising a data storage device controller for receiving a data storage device on which is provided the content, an authentication data storage device for storing authentication data, a data port connectable to a host device so that the apparatus can be placed into electronic communication with the host device, and a communications hub to mediate electronic communication between the data storage device controller, the authentication data storage device and the data port, wherein the apparatus is configured to permit content provided on the data storage device to be outputted from the data port according to the authentication data.

WO 2004/081706 A2

MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND APPARATUS FOR CONTROLLING THE PROVISION OF DIGITAL CONTENT

FIELD OF THE INVENTION

The present invention relates to a digital security method and apparatus, of particular but by no means exclusive application in controlling the distribution of electronic content such as software (and, in one particular example, software drivers), the distribution of digital content or media with copy protection, digital personal identification devices (typically carrying personal identity and other data), data management and portable devices for the secure storage of electronic content (such as data or software).

BACKGROUND OF THE INVENTION

Software including software drivers are presently commonly distributed with corresponding hardware on computer readable media such as CD-ROM, or over the Internet. These approaches, however, require the provision of such media or an Internet connection, both restrictions on the portability of the hardware.

Currently techniques exist for preventing the copying of digital content on music CDs, but few particular effective approaches exist for digital media such as floppy diskettes, zip diskettes, CD-ROMs and USB-flash devices.

In the field of smart cards and other devices for storing personal data or for data management, techniques such as the use of secret keys and digital certificates are presently employed to identify a person's identity. Personal Digital Assistants (PDAs) carry personal information but are not generically designed to prove a person's identity. No such device exists that combines the storage of a person's identity with personal information such as electronic mail.

There also exist a number of mass storage USB tokens, including that of Trek Technology (Singapore) Pte Ltd as described in WO 01/61692. Further, WO 00/42491 (Rainbow Technologies Inc) describes a cryptographic USB token.

Existing approaches for the portable secure storage of digital data also include the encryption of files on diskettes.

SUMMARY OF THE INVENTION

The present provides, in a first broad aspect, an apparatus for controlling the provision of digital content, comprising:

a data storage device controller for receiving a data storage device on which is provided said content;

an authentication data storage device for storing authentication data;

a data port connectable to a host device so that said apparatus can be placed into electronic communication with said host device; and

a communications hub to mediate electronic communication between said data storage device controller, said authentication data storage device and said data port;

wherein said apparatus is configured to permit content provided on said data storage device to be outputted from said data port according to said authentication data.

Preferably said data storage device is a non-volatile data storage device. More preferably said data storage device is a flash memory device. In these embodiments, the data storage device controller is preferably a controller suitable for the respective device.

Thus, content (which could comprise software, audio,

video, personal or other information, etc.) can be provided on the data storage device (such as a flash memory device, for example a flash card), but only copied to the data port (and thence to, for example, a computer or a playback device) if a suitable correspondence exists between the authentication data and the content. For example, the content may be configured to be read from the data storage device only if a particular password, security key or digital certificate is provided: that password or security key would be stored as the authentication data on the authentication data storage device. The authentication data storage device could take any suitable form, as will be understood by those in the art, such as a smart card chip or a biometric device.

It should be understood, however, that the apparatus - though configured to permit content provided on said data storage device to be outputted from the data port according to said authentication data - may be configured so that this outputting is limited in a predetermined way. Thus, the data storage device may include a first storage portion for storing at least one software viewer or player for viewing or playing said content, and a second storage portion for storing said content, wherein said apparatus is configured to permit the accessing of said software viewer or player and of said content (such as by a computer when said apparatus is connected to that computer) such that said content can be viewed or played by means of said software viewer or player without allowing said content to be copied (such as to another device, storage medium or printer).

Preferably the apparatus includes a cryptographic processor that is operable to encrypt or decrypt said content by means of at least one cryptographic key stored in said authentication data storage device. The cryptographic key may comprise or be derived from the

authentication data.

Thus, the authentication data (whether comprising a password, a secret key and/or a digital certificate, or otherwise) can additionally be used for encryption and copy protection, and the apparatus is preferably operable to encrypt and/or decrypt said content on the basis of the authentication data (i.e. using the authentication data as a cryptographic key, or deriving a cryptographic key from the authentication data).

The authentication data storage device may also comprise a combination of secure microcontrollers and EEPROM chips.

The invention thereby provides an apparatus that can be used as both a mass storage token and as a cryptographic token (the latter preferably in the form of a cryptographic processor).

Preferably said communications hub comprises a Universal Serial Bus (USB) hub.

Preferably the data port comprises a USB connector.

In one embodiment, said content comprises software.

In another embodiment, said content comprises software device drivers.

Preferably said apparatus includes a communications port for connecting said apparatus to a hardware device associated with said content.

Alternatively, said apparatus is provided in a hardware device and in electronic communication with said hardware device.

Thus, the hardware device would typically be a hardware peripheral that the software device drivers will be working with. The data storage device is then used to contain the software drivers for the hardware device, or digital media, personal data and other data to be secured. The authentication data storage device can then also store unique secret keys for identifying the hardware device and/or for ensuring the authenticity and originality of the hardware.

In another embodiment, when the content comprises digital media for distribution with copy protection, the data storage device contains software portions or drivers for reading, displaying or playing said digital media.

Thus, these software components would typically be designed to prevent unauthorized duplication of the digital media stored on the data storage device by using techniques such as encryption and capturing operating system functions.

In one embodiment, further authentication data is stored on said data storage device.

Thus, for data management (such as of personal data), the content comprises software modules for the host device that are designed to be incorporated into software applications so that personal identity data, such as secret keys and digital certificates, may be stored in the data storage device as well as in the authentication data storage device. Other personal data, such as email and personal calendar, can be stored in the data storage device.

In another embodiment, for portable secure storage of digital data, the data storage device contains said digital data in encrypted form while the authentication

data storage device contains secret keys for the encryption.

In all the applications above, the data in the data storage device may be in clear or in encrypted form, depending on the application.

The present also provides, in a second broad aspect, a method for controlling the provision of digital content, comprising:

providing said content on a data storage device readable by means of a data storage device controller;

providing authentication data on an authentication data storage device;

placing said data storage device controller and authentication data storage device in data communication with a host device;

controlling the provision of said content to said host device according to at least said authentication data.

The present provides, in a third broad aspect, a method for controlling access to digital content, comprising:

providing said content on a computing or other electronic device;

providing authentication data and control software on an authentication apparatus comprising:

a control software storage device controller for receiving a control software storage device on which is provided control software;

an authentication data storage device for storing authentication data;

a data port connectable to said computing or other electronic device so that said apparatus can be placed into electronic communication with said computing or other electronic device; and

a communications hub to mediate electronic

communication between said authentication data storage device controller, said authentication data storage device and said data port;

wherein said apparatus is configured to permit said control software provided on said control software storage device storage device to be used to control application software on said computing or other electronic device according to said authentication data.

The electronic device could be a computer peripheral, such as a printer, a scanner or a digital camera. By this means, the software drivers can be distributed with the electronic device itself, rather than on a separate CD-ROM or the like.

Preferably the authentication apparatus includes a cryptographic processor that is operable to encrypt or decrypt said content by means of at least one cryptographic key stored in said authentication data storage device. More preferably, the cryptographic key comprises or is derived from the authentication data.

BRIEF DESCRIPTION OF THE DRAWINGS

In order that the present invention may be more clearly ascertained, preferred embodiments will now be described, by way of example, with reference to the accompanying drawing, in which:

Figure 1 is a schematic diagram of an apparatus for distributing content associated with a hardware device according to a preferred embodiment of the present invention, together with the hardware device;

Figure 2 is a schematic diagram of an apparatus for distributing software device drivers associated with a hardware device according to another preferred embodiment of the present invention, together with the hardware device;

Figure 3 is a schematic diagram of an apparatus

for distributing digital storage media with copy protection according to a further preferred embodiment of the present invention;

Figure 4 is a schematic diagram of an authentication apparatus for personal identity and data management and for portable secure storage of digital data according to another preferred embodiment of the present invention;

Figure 5 is a schematic diagram of a system for centrally programming and managing the apparatus of figure 4; and

Figure 6 is a perspective view of an example of the apparatus of figure 4.

DETAILED DESCRIPTION OF THE DRAWINGS

An apparatus 10 for distributing digital content associated with a hardware device according to an embodiment of the present invention, together with the hardware device 12, is shown in figure 1.

The apparatus 10 comprises a Universal Serial Bus (USB) hub 14, an authentication device in the form of a smart card chip 16 or a biometric device 18, a flash controller 20 for reading flash memory 22 and a USB connector 24.

The authentication device 16,18 and the flash controller 20 communicate via USB hub 14 with a host device (not shown: typically a computer) by means of USB connector 24. The apparatus 10 is in fact incorporated within the hardware device 12 and connected thereto by means of a further USB connector (not shown) to the USB hub 14. The USB hub 14 in this embodiment will typically be the USB hub of the hardware device 12 itself.

The content on flash memory 22 (provided with the hardware device 12) to the host device is permitted only if the correct and corresponding authentication data is detected

on the authentication device 16,18.

Particular examples of applications of this approach are given below by reference to figures 2 to 4.

(1) Software Driver Distribution

Figure 2 is a schematic diagram of an apparatus 30 for distributing software device drivers associated with a hardware device according to an embodiment of the present invention, together with the hardware device 32.

The apparatus 30 comprises USB hub 34, an authentication device in the form of a smart card chip 36, a flash controller 40 for reading flash memory 42 and a USB connector 44. Flash memory 42 contains the content (here in the form of the software device drivers for hardware device 32) that are needed for the operating system of the host device (not shown, but connected at USB connector 44) to operate with the hardware device 32. The hardware device 32 could be a computer peripheral such as a printer, or scanner, or it could represent a smart card that itself acts as the authentication device.

The smart card chip 36 contains secret keys, etc., for establishing authenticity of the hardware device 32 and the software device driver: the software device driver performs authentication with the smart card chip 36 to ensure that the device driver has not been modified and the hardware device 32 is original.

(2) Digital Media Distribution with Copy Protection

Figure 3 is a schematic diagram of an apparatus 50 for distributing digital storage media with copy protection according to an embodiment of the present invention. The content in this example may be digitized music and video such as MP3 and MPEG or software packages.

The apparatus 50 comprises USB hub 54, an authentication device in the form of a smart card chip 56, a flash controller 60 for reading flash memory 62 and a USB connector 64. Flash memory 62 contains the content, in this example in the form of audio/video digital content to be distributed, and software applications to view, play and install the content on the host device (not shown, but connected at USB connector 64).

The content stored in the flash memory 62 is in encrypted form to prevent unauthorized duplication. Software viewers, players or installers also reside in the flash memory. The viewers, players and installers are written in a way that they only allow the media and applications to be viewed, played or installed, but do not allow them to be duplicated. Strong cryptographic protocols are used in these viewers, players and installers to prevent unauthorized duplication.

The smart card chip 56 contains secret keys or other parameters to prove the authenticity and originality of the media. Other information regarding the number of times a digital data has been accessed or the identity of the computer or player can be recorded in the smart card chip. This allows the number of times or the location the digital data or the software package has been accessed or installed can be restricted.

(3) Personal Identity and Data Management and Portable Secure Storage of Digital Data

Figure 4 is a schematic diagram of an authentication apparatus 70 for personal identity and data management and for portable secure storage of digital data in the form of personal identity data according to an embodiment of the present invention. The authentication data is in the form of personal identity data such as digital certificates and passwords while the content (or personal data) could be

electronic mail, personal documents, passwords, and other data.

The apparatus 70 comprises USB hub 74, an authentication device in the form of a smart card chip 76, a flash controller 80 for reading flash memory 82 and a USB connector 84. Flash memory 82 contains the content which, as mentioned above, in this example is in the form of electronic mail, personal documents, passwords and other data.

The flash memory 82 is used to store these data in clear or encrypted form. The more sensitive data (together with the digital certificates or passwords for proving identity or the secret keys used to sign, encrypt and decrypt the data in the flash card 82) is securely stored in the smart card chip 76.

Digital certificates are used for secure computer applications such as secure email (S/MIME) and secure internet connection (Secure Socket Layer, SSL), for signing and encrypting email.

Figure 5 is a schematic diagram of a system 90 for centrally programming and managing the authentication apparatus 70 of figure 4, in use with such the authentication apparatus 70 and a computer network 92.

The system 90 comprises a central management system 94 and a programmer 96. The programmer 96 includes a USB port for connecting to the USB port of USB connector 84 of authentication apparatus 70, so that the system 90 can be used to program each such authentication apparatus 70 by installing in an authentication apparatus 70 keys belonging to each user.

The keys are held in a Public Key Depository 98, which

holds such keys for secure applications such as S/MIME. The Public Key Depository 98 is accessible by the central management system 94 by computer network.

The system 90 installs - into the flash memory 82 of each authentication apparatus 70 - installation and configuration programs for subsequently configuring the software applications on networked computers 100 (each running secure applications such as S/MIME) on computer network 92; a user can take an authentication apparatus that has been programmed in this manner (such as authentication apparatus 70') and use it to gain ready access to those applications on any of computers 100. This enables each user to use these applications easily without the necessity of a system administrator installing applications or performing configuration for the user. The user also does not need to carry along another medium (such as an installation disk), and is free to perform this installation at all the computers that the user is authorized to use.

This convenience for the user is enabled by the flash storage space, in addition to the smart card chip, the latter of which is responsible for the key storage.

This system thus reduces the complexity of deployment by incorporating all the installation program and information within the device itself.

Figure 6 is a perspective view of an example of an authentication apparatus 102 according to this embodiment (such as authentication apparatus 70 of figures 4 and 5). As is apparent in this figure, the authentication apparatus 102 includes a UBS plug 104 (for plugging into a USB port) and a body 106 that encases the data storage and processing components of the apparatus. The apparatus 102 is designed to be hand-held, so it is of appropriate

dimensions and provided with finger grips 108 for ease of manipulation.

Thus, the present invention allows device drivers to be distributed together with the hardware device itself, and for a single architecture to be used for multiple applications.

Modifications within the scope of the invention may be readily effected by those skilled in the art. It is to be understood, therefore, that this invention is not limited to the particular embodiments described by way of example hereinabove.

In the claims that follow and in the preceding description of the invention, except where the context requires otherwise owing to express language or necessary implication, the word "comprise" or variations such as "comprises" or "comprising" is used in an inclusive sense, i.e. to specify the presence of the stated features but not to preclude the presence or addition of further features in various embodiments of the invention.

CLAIMS:

1. An apparatus for controlling the provision of digital content, comprising:

a data storage device controller for receiving a data storage device on which is provided said content;

an authentication data storage device for storing authentication data;

a data port connectable to a host device so that said apparatus can be placed into electronic communication with said host device; and

a communications hub to mediate electronic communication between said data storage device controller, said authentication data storage device and said data port;

wherein said apparatus is configured to permit content provided on said data storage device to be outputted from said data port according to said authentication data.

2. An apparatus as claimed in claim 1, wherein said apparatus includes a cryptographic processor that is operable to encrypt or decrypt said content by means of at least one cryptographic key stored in said authentication data storage device.

3. An apparatus as claimed in claim 2, wherein said cryptographic key comprises or is derived from said authentication data.

4. An apparatus as claimed in any one of the preceding claims, wherein said data storage device includes a first storage portion for storing at least one software viewer or player for viewing or playing said content, and a second storage portion for storing said content, wherein said apparatus is configured to permit the accessing of said software viewer or player and of said content such

that said content can be viewed or played by means of said software viewer or player without allowing said content to be copied.

5. An apparatus as claimed in any one of the preceding claims, wherein said authentication data storage device comprises a combination of secure microcontrollers and EEPROM chips and said data storage device is a flash memory device.

6. An apparatus as claimed in any one of the preceding claims, wherein said communications hub comprises a Universal Serial Bus hub.

7. An apparatus as claimed in any one of the preceding claims, wherein said data port comprises a Universal Serial Bus connector.

8. An apparatus as claimed in any one of the preceding claims, wherein said content comprises software.

9. An apparatus as claimed in any one of preceding claims, wherein said content comprises software device drivers.

10. An apparatus as claimed in any one of preceding claims, including a communications port for connecting said apparatus to a hardware device associated with said content.

11. An apparatus as claimed in any one of preceding claims, wherein said apparatus is provided in a hardware device and in electronic communication with said hardware device.

12. An apparatus as claimed in claim 1, wherein said content comprises digital media for distribution with copy

protection, and said data storage device contains software portions or drivers for reading, displaying or playing said digital media.

13. An apparatus as claimed in claim 1, wherein further authentication data is stored on said data storage device.

14. A method for controlling the provision of digital content, comprising:

providing said content on a data storage device readable by means of a data storage device controller;

providing authentication data on an authentication data storage device;

placing said data storage device controller and authentication data storage device in data communication with a host device;

controlling the provision of said content to said host device according to at least said authentication data.

15. A method as claimed in claim 14, including encrypting or decrypting said content by means of at least one cryptographic key stored in said authentication data storage device.

16. A method as claimed in claim 15, wherein said cryptographic key comprises or is derived from said authentication data.

17. A method for controlling access to digital content, comprising:

providing said content on a computing or other electronic device;

providing authentication data and control software on an authentication apparatus comprising:

a control software storage device controller for receiving a control software storage device

on which is provided control software;

an authentication data storage device for storing authentication data;

a data port connectable to said computing or other electronic device so that said authentication apparatus can be placed into electronic communication with said computing or other electronic device; and

a communications hub to mediate electronic communication between said authentication data storage device controller, said authentication data storage device and said data port;

wherein said authentication apparatus is configured to permit said control software provided on said control software storage device storage device to be used to control application software on said computing or other electronic device according to said authentication data.

18. A method as claimed in claim 17, wherein said authentication apparatus includes a cryptographic processor that is operable to encrypt or decrypt said content by means of at least one cryptographic key stored in said authentication data storage device.

19. A method as claimed in claim 18, wherein said cryptographic key comprises or is derived from said authentication data.

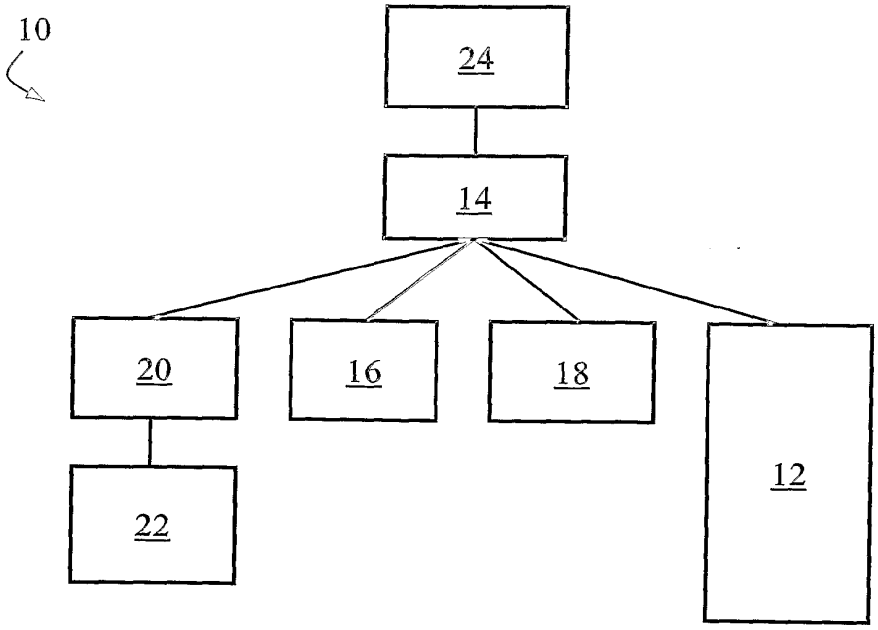


Figure 1

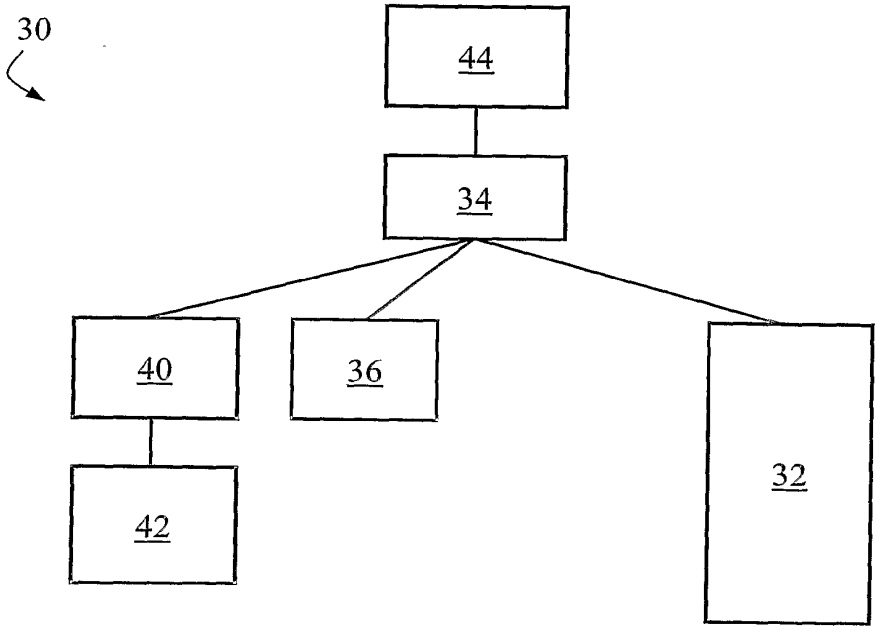


Figure 2

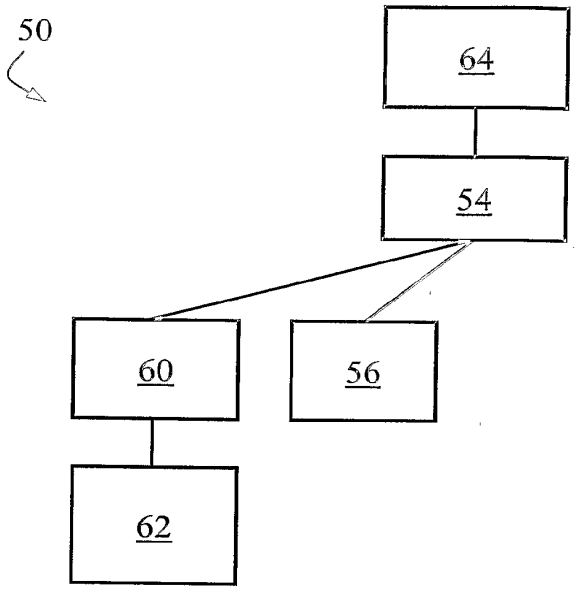


Figure 3

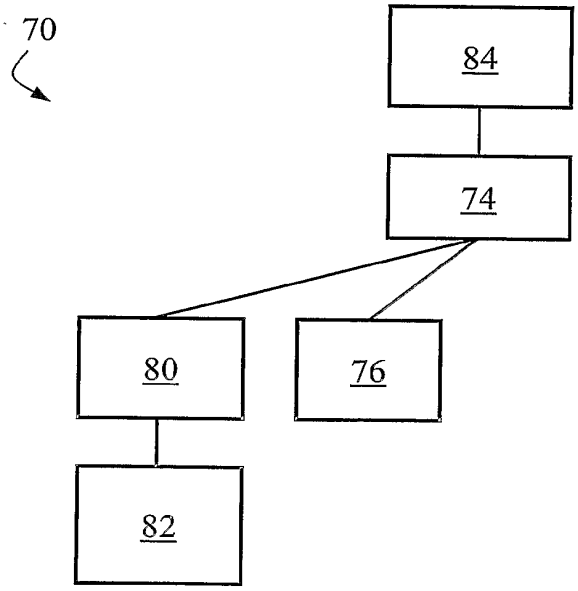


Figure 4

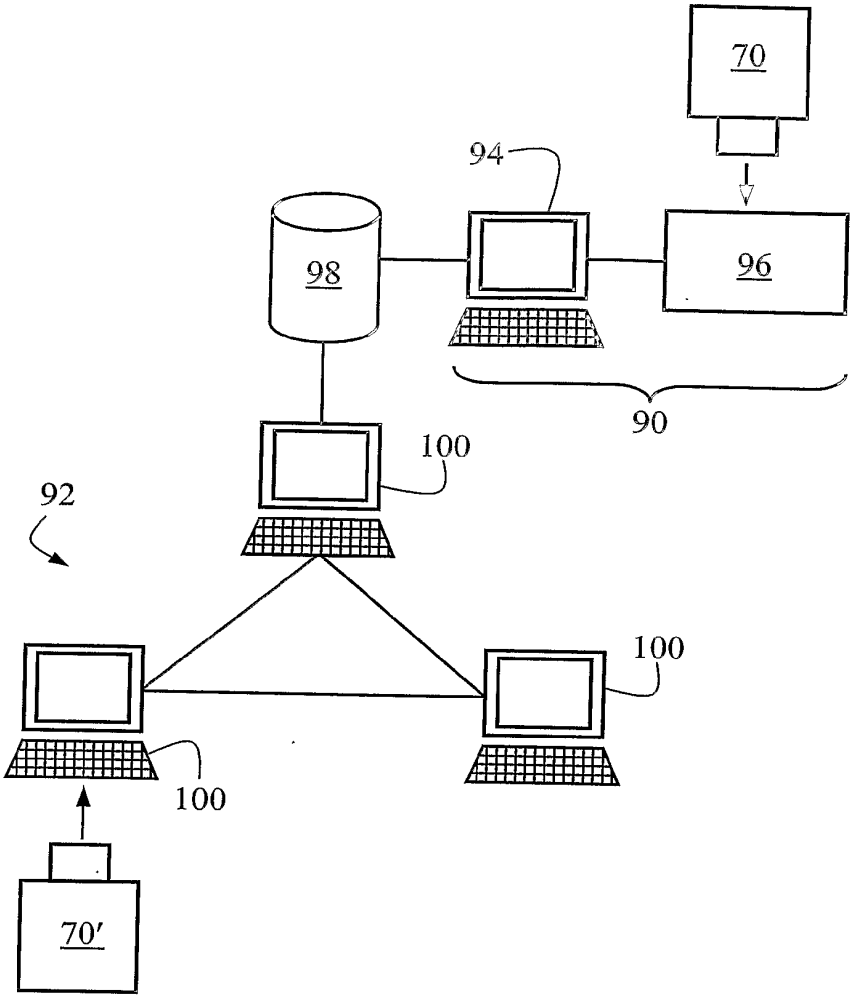


Figure 5

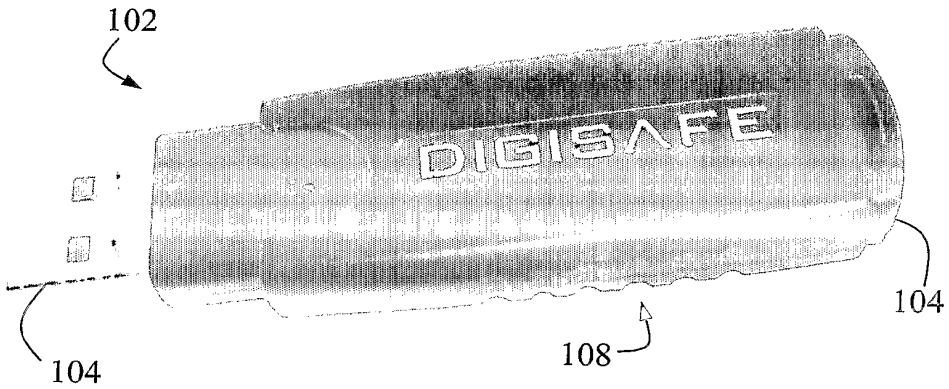


Figure 6

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 September 2004 (23.09.2004)

PCT

(10) International Publication Number
WO 2004/081769 A1

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number:
PCT/IB2004/000738

(22) International Filing Date: 12 March 2004 (12.03.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03290655.4 14 March 2003 (14.03.2003) EP

(71) Applicant *(for all designated States except US)*: **AXALTO SA** [FR/FR]; 36-38 rue de la Princesse, BP 45, F-78431 Louveciennes (FR).

(71) Applicant *(for MC only)*: **SCHLUMBERGER MALCO INC** [US/US]; 9800 Reistertown, OwinG Mills, Owing Mills, MD 21117 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **AKKAR, Mehdi-Laurent** [FR/FR]; 17 Rue Lafouge, F-94250 Gentilly (FR).

(74) Common Representative: **SCHLUMBERGER SYSTEMES**; C/O Patrice GUILLERM, 36-38 rue de la Princesse, BP 45, F-78431 Louveciennes (FR).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

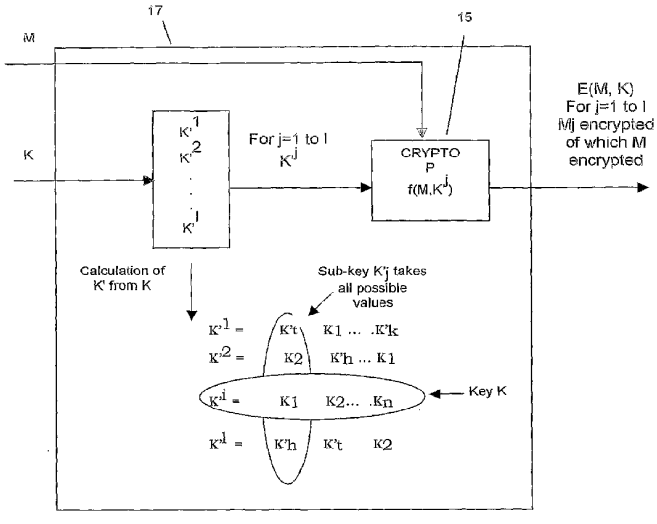
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv)) for US only*

Published:
— *with international search report*

[Continued on next page]

(54) Title: PROCESS OF SECURITY OF A UNIT ELECTRONIC UNIT WITH CRYPTOPROCESSOR



(57) Abstract: The invention concerns a process for securing an electronic device incorporating a hardware component capable of autonomous implementation of calculation process f using one key K. the process involves calculating at least two new keys K^i such that at least one of said new keys is identical to key K, and one of said new keys is different from key K, and executing said calculation process f successively with each of said calculated keys K^i, using said hardware component.

WO 2004/081769 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

PROCESS OF SECURITY OF A UNIT ELECTRONIC WITH CRYPTOPROCESSOR

The invention concerns a process for securing an electronic device incorporating a hardware component such as a cryptoprocessor, for the purpose of autonomous implementation of a cryptographic algorithm using a secret quantity such as a secret key. In more precise terms, the process is designed to secure said cryptoprocessor against a certain type of physical attacks referred to as Differential Power Analysis (first order electronic attacks or higher) which seek to obtain information concerning the secret key by studying the power consumption of the electronic device during execution of calculations.

TECHNICAL DOMAIN

Certain components incorporate a hardware DES algorithm. The DES algorithm has the advantage of being extremely fast – of the order of 20 microseconds – and can apparently withstand SPA and DFA type attacks. Unfortunately, it cannot withstand a first order DPA attack. Indeed, with a reasonable number of samples – of the order of 10,000 – it is possible to extract the key. Faced with this vulnerability, it can be necessary to reprogram a secure software DES in full.

One purpose of this invention is to propose a process and system for securing components incorporating cryptoprocessors or equivalent devices, in particular against DPA type attacks.

The cryptographic algorithms considered here use a secret key to calculate output information according to input information. This can involve an encryption, decryption, signature or signature verification, authentication or non-repudiation operation. The

CONFIRMATION COPY

IPR2022-00412
Apple EX1053 Page 831

algorithms are constructed in such a way that an attacker with knowledge of the inputs and outputs, cannot in practice deduce any information concerning the secret key itself. Numerous applications base their security on secret key cryptographic algorithms such as the DES, or the more recent AES algorithm, which has now taken its place as the world-wide encryption standard (see John Daemen, Vincent Rijmen; AES proposal; Rijndael: http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf).

We are interested in a broader class than that traditionally designated by the expression *secret key algorithm* or *symmetrical algorithm*. In particular, all that is described in this patent application also applies to the so-called public key or asymmetrical algorithms, which in fact incorporate two keys, one public and the other private and not disclosed, the latter being the target for the attacks described below.

The Power Analysis type attacks described by Paul Kocher and Cryptography Research (see document "Introduction to Differential Power Analysis and Related Attacks" by Paul Kocher, Joshua Jaffe and Benjamin Jun, Cryptography Research, 870 Market St., Suite 1008, San Francisco, CA 94102, HTML version of the document accessible at URL address: http://www.cryptography.com/dpa/technical/index.html, mentioned in this application for reference purposes) are based on the observation that, in reality, the attacker can acquire information other than simple input and output data, on execution of calculations, such as the power consumption of the microcontroller or the electromagnetic radiation emitted by the circuit, for example. This information, which depends on secret quantities such as the key, leaks from the card.

Differential Power Analysis, abbreviated to DPA, is an attack which makes it possible to obtain information concerning the secret

IPR2022-00412
Apple EX1053 Page 832

key contained in the electronic device, by making a statistical analysis of records of power consumption for a large number of calculations with the same key.

We can consider, as a non-exhaustive example, the case of the DES (Data Encryption Standard) algorithm, a description of which can be found in any of the following documents:

FIPS PUB 46-2, Data Encryption Standard, 1994;

FIPS PUB 74, Guidelines for Implementing and Using the NBS Data Encryption Standard, 1981;

ANSI X3.92, American National Standard, Data Encryption Algorithm, 1981;

ISO/IEC 8731:1987, Banking - Approved Algorithms for Message Authentication - Part 1: Data Encryption Algorithm (DEA).

Or in the following work:

Bruce Schneier, Applied Cryptography, 2nd edition, John Wiley & Sons, 1996, page 270.

The above-mentioned documents are indicated in this application for reference purposes.

The DES algorithm is executed in 16 steps referred to as rounds (see Figure 1a). In each of these 16 rounds, conversion F is executed on 32 bits. This conversion F uses eight 6-bit to 4-bit non-linear conversions, each coded in a table referred to as an S-box (see Figure 1b), where the S-boxes are noted S1, S2, ..., S8.

A DPA attack on the DES algorithm can be implemented as follows:

1st step: Consumption is measured on the first round for 1,000 DES calculations. The input values for these 1,000 calculations are noted E[1], ..., E[1000]. The 1,000 curves corresponding to power consumption measured for these calculations are noted C[1], ..., C[1,000]. Mean curve CM is also calculated for the 1,000 consumption curves.

IPR2022-00412
Apple EX1053 Page 833

2nd step: We consider the first output bit from the first S-box on the first round, for example. The value of this bit is noted b. It is easy to see that b only depends on 6 bits of the secret key. The attacker makes an assumption concerning the 6 bits concerned. The attacker calculates the theoretical values expected for b from these 6 bits and the E[i]. This makes it possible to separate the 1,000 inputs E[1], ..., E[1,000] into two categories: those which give b=0, and those which give b=1.

3rd step: Mean value CM' is then calculated for the curves corresponding to the first category inputs, namely those for which b=0. If CM and CM' show a marked difference, it is considered that the values adopted for the 6 bits of the key were correct. If CM and CM' do not show a marked difference in the statistical sense, namely no difference substantially greater than the typical variance for the noise measured, the 2nd step is repeated with a different selection for the 6 bits.

4th step: Steps 2 and 3 are repeated with a target bit b from the second S-box, and then from the third S-box, and so on up to the eighth S-box. Forty-eight bits of the secret key are finally obtained in this way.

5th step: The 8 remaining bits can be found by exhaustive search.

This attack requires no knowledge concerning the individual power consumption of each instruction, nor the position in time of each of these instructions. It applies in the same way if we assume that the attacker knows the outputs of the algorithm and corresponding consumption curves. It is based solely on the following fundamental assumption:

Fundamental assumption: An intermediate variable exists, appearing during the course of calculation of the algorithm, such that knowledge of a few key bits, in practice less than 32 bits, is sufficient to decide whether two inputs, respectively two outputs, give the same

value for this variable or not.

All algorithms using the S-box principle, such as the DES algorithm, are potentially vulnerable to DPA attack, as the customary methods of implementation generally lie within the framework of the assumption mentioned above.

So-called High-Order Differential Power Analysis attacks, abbreviated to HO-DPA, correspond to generalisation of the DPA type attack described above. They can use a number of different information sources apart from consumption, and can involve measurement of electromagnetic radiation, temperature, etc., and employ more sophisticated statistical processing than the simple notion of average, with less elementary intermediate variables (generalising bit b defined above). Nevertheless, they are based on precisely the same fundamental assumption as the DPA attack.

IPR2022-00412
Apple EX1053 Page 835

SUMMARY OF THE INVENTION

The invention concerns a process for securing an electronic device incorporating a hardware component capable of autonomous implementation of a calculation process using key K, characterised by the fact that it involves calculating at least two new keys K'^i such that for at least one given i=j, $K'^j=K$ and for at least one i=t, $K'^t <> K$, and executing said calculation process with each of said calculated keys K'^i in succession, using said hardware component.

According to one particular form of implementation, the process involves calculating I=α m new keys K'^1, ..., K'^l, so that for a given j (0<j<n+1), sub-keys K'^i_j (0<i<l+1) take all the possible values, including the value of sub-key Kj, and executing hardware cryptographic function f with these I new keys K'^1, ..., K'^l, in a random manner.

The invention also concerns an electronic device and a smart card for example, and a program for implementation of the process.

BRIEF DESCRIPTION OF THE DRAWINGS

Other purposes, advantages and characteristics of the invention will emerge from the following description of implementation of the process according to the invention, and of a method of execution of an electronic device adapted for this implementation, given for non-exhaustive example purposes referring to the appended drawings where:

- Figure 1 shows an electronic device according to the invention in schematic form;

- Figure 2 shows a hardware component of said device according to Figure 1 in schematic form;
- Figure 3 shows the process according to the invention in schematic form.

IMPLEMENTATION OF THE INVENTION

The process according to the invention is designed to secure an electronic device, for example an on-board system such as a smart card implementing a cryptographic calculation process which uses a secret key. The electronic device incorporates means to process information, such as a processor, and means to store information such as a memory.

As a non-exhaustive example, the electronic device described below corresponds to an on-board system incorporating electronic module 1 as shown in Figure 1. Modules of this type usually take the form of a monolithic integrated electronic microcircuit or chip, which, once protected physically by any known means, can be mounted on a portable object such as a smart card, microcircuit card or other which can be used in various domains, for example.

Microprocessor electronic module 1 comprises CPU microprocessor 3, connected bidirectionally via internal bus 5 to a non-volatile memory 7 of the ROM, EEPROM, Flash, FeRam or other type containing an executable program, RAM memory 11, I/O device 13 for communication with the exterior, and cryptoprocessor calculation unit 15 (CRYPTO P), this component being capable of autonomous cryptographic calculation, such as calculation of a DES algorithm, for example. As shown in Figure 2, cryptoprocessor 15 of said module 1 executes calculation process f using secret key K, stored in a secret zone of a memory, for example of the EEPROM type, on a message M.

IPR2022-00412
Apple EX1053 Page 837

We will firstly consider the solution in its general form. As shown in Figure 3, the objective is to calculate result E(M,K) of cryptographic function E on message M, using key K. For this purpose, we have function f, which, in its capacity as a black box, executes the same calculation as E but cannot withstand DPA attack in particular. We also consider that key K acts in regard to the algorithm in the form of n small sub-keys mb (taking mb<10 bits, or $m=2^{mb}$ possible values for each sub-key), which will then be noted K1,K2, ... , Kn, and which will be susceptible to DPA attack in particular. The sub-keys are of the same size in the form of implementation described below. The invention also applies for sub-keys of a different size.

The invention involves associating external software module 17 with the cryptoprocessor, to secure the cryptographic function implemented by said cryptoprocessor 15.

As shown in Figure 3, the invention involves calculating $I=\alpha$ m new keys K'^1, ..., K'^I, so that for a given j ($0<j<n+1$), each sub-key K'^i_j ($0<i<l+1$) takes all the possible values, and according to a special form of implementation α times, including the value of sub-key Kj, and executing hardware cryptographic function f with these I new keys K'^1, ..., K'^I in a random manner.

In other words, the idea is to execute $I = \alpha$ m successive calculations with keys K'^i, $0 \leq i < l$, such that:

there exists i such that $K'^i = K$.

For all the j, we have $\{ K'^i j, 0 \leq i<n \} = \{0,1, \ldots ,n-1\}$, with each sub-key appearing exactly α times.

This means in fact that we will execute a number of successive calculations with different keys (including the true key), in such a way that each possible sub-key appears the same number of times.

The calculations will also be executed in a random order. Consequently, the attacker has no chance of identifying the correct sub-key by DPA attack, as this sub-key appears neither more nor less frequently than any other.

We will now see how this countermeasure (noted CM in the following paragraphs) applies to different algorithms.

Simple application to the DES algorithm

Notations

We will adopt the following notations for the DES algorithm:
PC1 represents the initial permutation of the key, reducing the key from 64 to 56 bits.
IPC1 represents the inverse of PC1 (56 bits to 64), where the 8 missing bits are completed (parity bits are frequently used).
PC2 represents the combination of compressive permutation (56 bits to 48 bits) and shift of the key to the first round.
IPC2 represents the inverse of PC2 (48 to 56 bits), where the 8 undetermined bits (8=56-48) are selected arbitrarily (for example randomly).
The permutation from 48 bits to 64 bits (combination of IPC2 and IPC1) is noted PP.

We see that PP makes it possible, starting from key K48 with 48 bits, used in the first round of the DES algorithm, to reach global key K64 =PP(K48) having the following property: using K64 as the key for a DES calculation, we obtain K48 as the first sub-key in the first round.

We will now see how we can apply our countermeasure in concrete terms.

1.1 Initial implementation of the CM

In the case of the DES algorithm, the sub-keys are used in the form of n=8 sub-keys of mb=6 bits each, giving m=64 possibilities. We shall then execute 64 successive calculations (α =1) with the following derivative keys:

$K_{00} = K \oplus PP(\ 000000 \mid 000000 \mid \ldots \mid 000000 \mid 000000\ )$
$K_{01} = K \oplus PP(\ 000001 \mid 000001 \mid \ldots \mid 000001 \mid 000001\ )$
$K_{02} = K \oplus PP(\ 000010 \mid 000010 \mid \ldots \mid 000010 \mid 000010\ )$
$K_{03} = K \oplus PP(\ 000011 \mid 000011 \mid \ldots \mid 000011 \mid 000011\ )$
.
.
.
$K_{61} = K \oplus PP(\ 111101 \mid 111101 \mid \ldots \mid 111101 \mid 111101\ )$
$K_{62} = K \oplus PP(\ 111110 \mid 111110 \mid \ldots \mid 111110 \mid 111110\ )$
$K_{63} = K \oplus PP(\ 111111 \mid 111111 \mid \ldots \mid 111111 \mid 111111\ )$

It is thus easy to see that for each of the eight sub-keys used in the first round, the 64 possible values are represented equally, and that true key K00 is present in the list. It is then merely necessary to execute 64 DES calculations with the 64 derivative keys in a random order, and select the final result as being that where the correct key has been used.

This can be done in the following way. Sixteen memory bytes are allocated to store the result. An additional byte is also allocated for each Ki (initialised in this case at 0 or 8), which will indicate the byte from which the result is stored in memory. Thus, this byte will take the value 8 for all keys except K00 for which it will take the value 0. This makes it possible to use a relatively generic code, which could resemble the next pseudo-code C, considering that we have one

function executing a memory copy, one which calculates the PP(i | ... | i) and one which randomizes the 64 keys.

```
void
 DES_encrypt_DPA( unsigned char in[8],
                                  unsigned char cle[8],
                  unsigned char out[8] )
{
   int i;
   unsigned char M1[8], M2[16], K[64][9];

   memcopy(K[0],cle,8);
   K[0][8] = 0;

   for(i=1; i<64; i++)
   {
      memcopy(K[i], cle XOR PP(i | ... | i), 8);
      K[i][8] = 8;
   }

   randomize_0_63(K);

   for(i=0; i<64; i++)
   {
      memcopy(M1, in, 8);
      DES_encrypt_non_DPA(M1,K[i]);

      for(j=0;j<8;j++)
      {
         M2[K[i][8] + j] = M1[j];
      }
   }

   memcopy(out, M2, 8);
}
```

1.2 General security considerations

From the DPA point of view, it is easy to see that any attacker, unable to distinguish for each of the 64 executions of the DES algorithm whether the true key is concerned or not, cannot attack the algorithm with a conventional DPA. However, it must be remembered that programming of the method requires a very strict approach, as any analysis making it possible to distinguish – even rarely – the

correct key destroys the CM completely! Attention must therefore be paid to the following critical points:

- Randomization: this step shifts the true key to location $0 \leq i < 64$ which must be unknown to the exterior.
- Result copy (loop to j): here again, the two values (0 or 8), which would enable the attacker, if revealed, to know which DES algorithm uses the true key, are involved.

3.4 CM extensions and various aspects

- If we take a closer look at function PP, it is easy to see that it is not necessary to use the same value for the eight sub-keys, as was done previously, to mask the key. Taking sub-key i, it is merely necessary for the 64 possible values to appear. It is not necessary for the order of the 64 values to be the same for a given sub-key as for another sub-key! The only requirement is that the value 0 of the sub-key (for which the true sub-key is used) appears at the same time for the eight sub-keys, so that one of the 64 calculations gives the correct result. We can thus imagine a derivation of the following type:

$K_{00} = K \oplus PP(\ 000000 \mid 000000 \mid \ldots \mid 000000 \mid 000000\ )$
$K_{01} = K \oplus PP(\ 011000 \mid 001101 \mid \ldots \mid 001001 \mid 111100\ )$
$K_{02} = K \oplus PP(\ 010101 \mid 001111 \mid \ldots \mid 001011 \mid 010000\ )$
$K_{03} = K \oplus PP(\ 110011 \mid 100010 \mid \ldots \mid 000011 \mid 010010\ )$

$K_{61} = K \oplus PP(\ 101011 \mid 011100 \mid \ldots \mid 110001 \mid 101000\ )$
$K_{62} = K \oplus PP(\ 100111 \mid 101010 \mid \ldots \mid 000110 \mid 010111\ )$
$K_{63} = K \oplus PP(\ 001110 \mid 010111 \mid \ldots \mid 011100 \mid 110001\ )$

This merely requires a function which executes a random permutation of the values [1,63].

It should be noted that the fact that the mask (000000 | ... | 000000) always appears in the initial position does not represent a problem, as the derivative keys are then permutated randomly before being used. If we consider that we have a function PP2(i,val) which replaces the 6 bits of value val in the correct position for it to correspond to sub-key i, we then obtain the following pseudo-code C:

```
void
DES_encrypt_DPA(unsigned char in[8],
                unsigned char cle[8],
          unsigned char out[8] )
{
  int i,j;
  unsigned char M1[8], M2[16], K[64][9];

  memcopy(K[0],cle,8);
  K[0][8] = 0;

  for(i=0;i<64;i++)
  {
    memcopy(K[i],cle,8);
  }

  for(i=0; i<8; i++)
  {
    unsigned char Perm63[63];

    randomize_1_63(Perm63);
    for(j=1; j<64; j++)
    {
      K[j] = K[j] XOR PP2(i,Perm[j]);
    }
  }

  randomize_0_63(K);

  for(i=0; i<64; i++)
  {
    memcopy(M1, in, 8);
    DES_encrypt_non_DPA(M1,K[i]);

    for(j=0;j<8;j++)
    {
      M2[K[i][8] + j] = M1[j];
    }
  }
```

```
    memcopy(out, M2, 8);
}
```

- Randomization of the 64 derivative keys can be performed using the following conventional method (cf. Crypto'2002 or Akkar/Goubin article on HODPA attacks on the DES algorithm), which involves scanning the keys from 0 to 63 with index i, and exchanging the key with index i with a key with an index selected randomly between 0 and 63:

```
void
randomize(unsigned char table[64])
{
   int i, i_temp;
   unsigned char temp;

   for(i=0; i<64; i++)
   {
      table[i] = i;
   }

   for(i=0; i<64; i++)
   {
      i_temp = random() % 64;
      temp = table[i];
      table[i] = table[i_temp];
      table[i_temp] = temp;
   }
}
```

3.5 Other DES rounds

We have seen how to protect the first DES round against DPA attack. Where the DES is more vulnerable on the 16th round in the protocol used, a similar method can naturally be envisaged. Only function PP will change, and correspond to the key-scheduling for the 16th round! It is then possible to use 64 key masks which protect both the first and last rounds. The following 64 key mask keys possess this property:

0000000000000000 8444054405410000 410900B100033003
C54D05F505423003
0093420342004141 84D7474747414141 419A42B242037142
C5DE47F647427142
0021000000950C9C 8465054405D40C9C 412800B100963C9F
C56C05F505D73C9F
00B2420342954DDD 84F6474747D44DDD 41BB42B242967DDE
C5FF47F647D77DDE
2200300918288100 A644354D1D698100 630930B8182BB103
E74D35FC1D6AB103
2293720A5A28C041 A6D7774E5F69C041 639A72BB5A2BF042
E7DE77FF5F6AF042
2221300918BD8D9C A665354D1DFC8D9C 632830B818BEBD9F
E76C35FC1DFFBD9F
22B2720A5ABDCCDD A6F6774E5FFCCCDD 63BB72BB5ABEFCDE
E7FF77FF5FFFFCDE
18008800A0000321 9C448D44A5410321 590988B1A0033322
DD4D8DF5A5423322
1893CA03E2004260 9CD7CF47E7414260 599ACAB2E2037263
DDDECFF6E7427263
18218800A0950FBD 9C658D44A5D40FBD 592888B1A0963FBE
DD6C8DF5A5D73FBE
18B2CA03E2954EFC 9CF6CF47E7D44EFC 59BBCAB2E2967EFF
DDFFCFF6E7D77EFF
3A00B809B8288221 BE44BD4DBD698221 7B09B8B8B82BB222
FF4DBDFCBD6AB222
3A93FA0AFA28C360 BED7FF4EFF69C360 7B9AFABBFA2BF363
FFDEFFFFFF6AF363
3A21B809B8BD8EBD BE65BD4DBDFC8EBD 7B28B8B8B8BEBEBE
FF6CBDFCBDFFBEBE
3AB2FA0AFABDCFFC BEF6FF4EFFFCCFFC 7BBBFABBFABEFFFF
FFFFFFFFFFFFFFFF

Obviously, this countermeasure (or at least the critical parts) must be implemented in the assembler mode, so as to avoid introducing vulnerability due to unfamiliarity with the methods used by the compiler.

2. Application to the AES algorithm

Obviously, this method can apply in a similar way to the AES algorithm. This is even simpler to explain, as the first sub-key used – which is frequently the target – comprises the key with no other conversion! Another practical difference stems from the fact that the key occurs 8 bits by 8 bits. Thus, in the case of an AES algorithm with key and 128-bit message, we obtain key derivation and a

pseudo-code C as follows:

$K_{00} = K \oplus (00000000 \mid 00000000 \mid ... \mid 00000000 \mid 00000000)$
$K_{01} = K \oplus (00000001 \mid 00000001 \mid ... \mid 00000001 \mid 00000001)$
$K_{02} = K \oplus (00000010 \mid 00000010 \mid ... \mid 00000010 \mid 00000010)$
$K_{03} = K \oplus (00000011 \mid 00000011 \mid ... \mid 00000011 \mid 00000011)$
.
.
.
$K_{61} = K \oplus (11111101 \mid 11111101 \mid ... \mid 11111101 \mid 11111101)$
$K_{62} = K \oplus (11111110 \mid 11111110 \mid ... \mid 11111110 \mid 11111110)$
$K_{63} = K \oplus (11111111 \mid 11111111 \mid ... \mid 11111111 \mid 11111111)$

```
void
AES_encrypt_DPA( unsigned char in[16],
                                 unsigned char cle[16],
            unsigned char out[16] )
{
   int i;
   unsigned char M1[16], M2[32], K[256][17];

   memcopy(K[0],cle,16);
   K[0][16] = 0;

   for(i=1; i<256; i++)
   {
      memcopy(K[i], cle XOR (i | ... | i), 16);
      K[i][8] = 16;
   }

   randomize_0_255(K);

   for(i=0; i<256; i++)
   {
      memcopy(M1, in, 16);
      AES_encrypt_non_DPA(M1,K[i]);

      for(j=0;j<16;j++)
      {
         M2[K[i][16] + j] = M1[j];
      }
   }

   memcopy(out, M2, 16);
}
```

The only real difference is that key-scheduling for the AES algorithm is not linear, in contrast to the DES, except for the first

sub-key. Thus, if we wish to protect the last round by this method, a method similar to the DES cannot be considered. It is then necessary to store the set of 256 keys specific to a given key, instead of the key derivation plan.

5

3. Conclusion

We thus see that it is possible, by execution of 64 DES (or 256 AES) algorithms and a number of ancillary calculations, to protect a cryptographic algorithm (DES or AES, for example) against DPA attack by means of a rapid although unprotected brick. Sixty-four DES or 256 AES may appear long, nevertheless in practice these hardware operations take a practically negligible amount of time.

10

15

CLAIMS

1. Process for securing an electronic device incorporating a hardware component capable of autonomous implementation of calculation process f using key K, characterised by the fact that it involves calculating at least two new keys K'^i such that at least one of said new keys is identical to key K, and at least one of said new keys is different from key K, and executing said calculation process f successively with each of said calculated keys K'^i using said hardware component.

2. Process according to claim 1, characterised in that it involves executing said calculation process with said keys K'^i in a random order.

3. Process according to claim 1 or 2, characterised in that key K is sub-divided into sub-keys K_1, ..., K_n, and that there exists at least one i such that key K'^i is different from K for at least one sub-key K'^i_j.

4. Process according to one of claims 1 to 3, characterised in that key K is sub-divided into sub-keys K_1, ..., K_n, and that the procedure involves calculating $I=\alpha$ m new keys K'^1, ..., K'^I, where m represents the number of possible values for one of sub-keys K'^i_j of K'^i, in such a way that for a given j ($0<j<n+1$), sub-keys K'^i_j ($0<i<l+1$) take all the possible values, including the value of sub-key Kj of K.

5. Process according to claim 4, characterised in that sub-keys K'^i_j ($0<i<l+1$) take all the possible values α times.

6. Electronic device incorporating means to store a calculation process, means to execute said process and a hardware component capable of autonomous implementation of a calculation process using

IPR2022-00412
Apple EX1053 Page 848

key K, characterised in that it incorporates a software module associated with the hardware component, capable of calculating at least two new keys K^i, such that at least one of new said keys is identical to key K, and one of said new keys is different from key K, and in that the software module is associated with the hardware component in such a way as to be able to transmit in succession to said hardware component, the new keys calculated to implement said calculation process with each of said new keys K^i.

7. Electronic device according to claim 6, characterised in that said software module transmits in succession the new keys calculated in a random order.

8. Computer program incorporating program code instructions for execution of the steps of the process according to one of claims 1 to 5, when said program is executed in an electronic device.

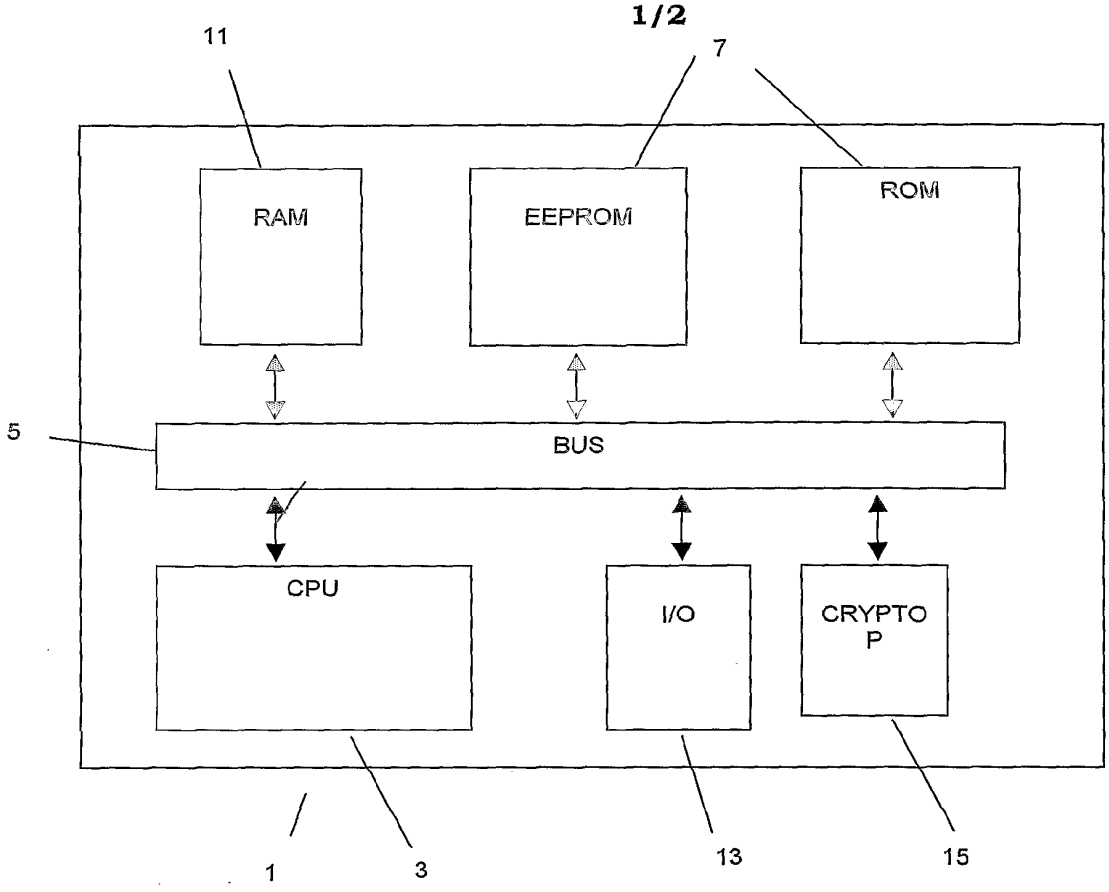

11
7
RAM
EEPROM
ROM
5
BUS
CPU
I/O
CRYPTO
P
1
3
13
15

FIG. 1

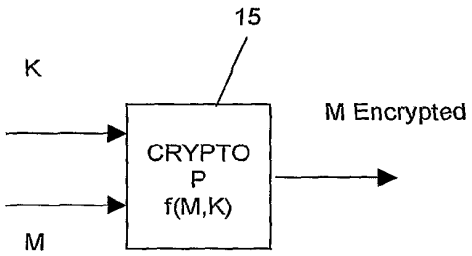

15
K
M Encrypted
CRYPTO
P
f(M,K)
M

FIG. 2

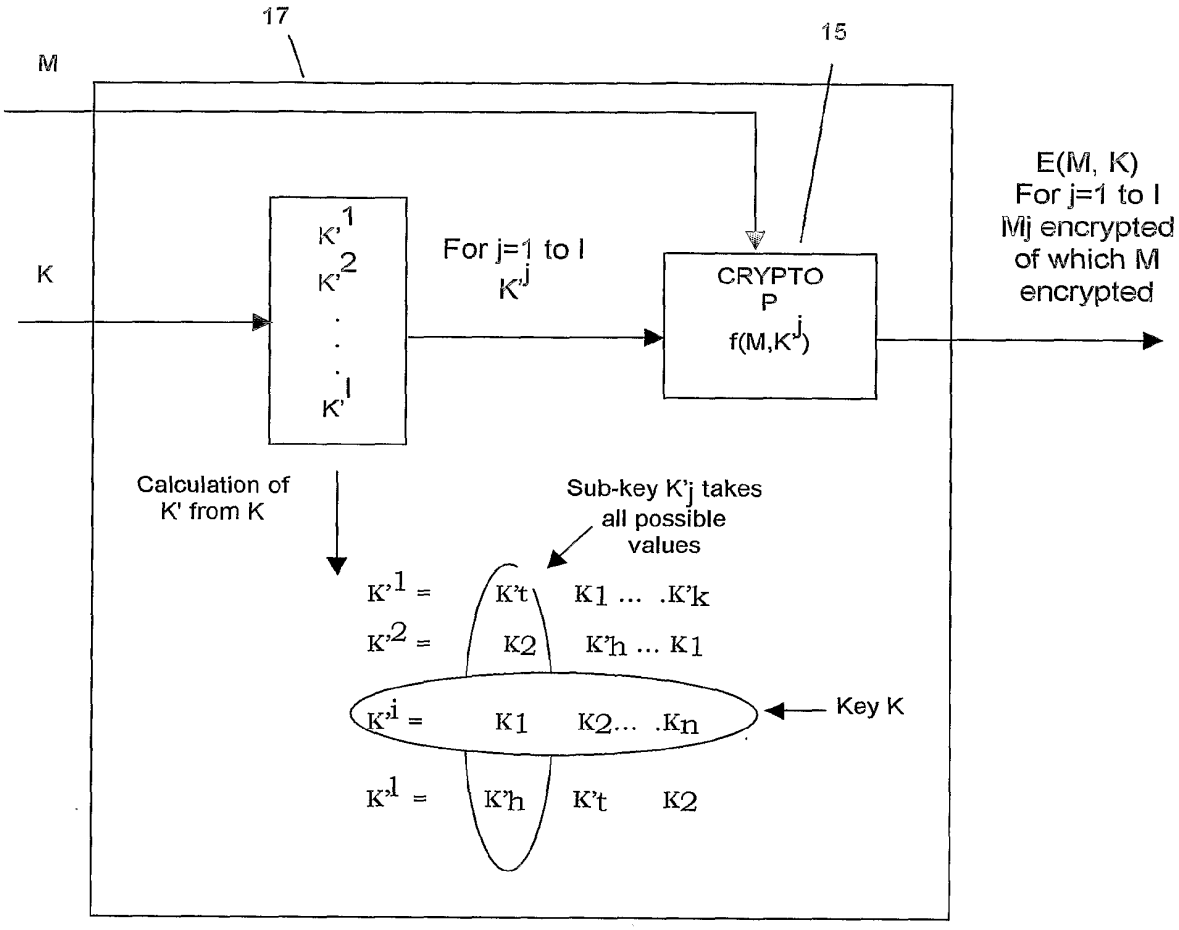

17
15
M
K
K'1
K'2
K'l
For j=1 to l
K'j
CRYPTO
P
f(M,K'j)
E(M, K)
For j=1 to l
Mj encrypted
of which M
encrypted
Calculation of
K' from K
Sub-key K'j takes
all possible
values
K'1 = K't K1 ... .K'k
K'2 = K2 K'h ... K1
K'i = K1 K2... .Kn
Key K
K'l = K'h K't K2

FIG. 3

INTERNATIONAL SEARCH REPORT

Int ional Application No
PCT/IB2004/000738

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01/31422 A (VON WILLICH MANFRED) 3 May 2001 (2001-05-03) page 3, line 11 - line 37 page 5, line 26 - page 6, line 37 page 8, line 27 - page 9, line 20 page 11, line 17 - line 29 page 12, line 7 - line 14 claims 1,3 figures 8,9 ----- -/--	1-8

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 July 2004	05/08/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Bichler, M

Form PCT/ISA/210 (second sheet) (January 2004)

IPR2022-00412
Apple EX1053 Page 852

INTERNATIONAL SEARCH REPORT

In onal Application No
PCT/IB2004/000738

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CHARI S ET AL: "TOWARDS SOUND APPROACHES TO COUNTERACT POWER-ANALYSIS ATTACKS" ADVANCES IN CRYPTOLOGY. CRYPTO '99. 19TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. SANTA BARBARA, CA, AUG. 15 - 19, 1999. PROCEEDINGS, LECTURE NOTES IN COMPUTER SCIENCE;VOL. 1666, BERLIN: SPRINGER, DE, 1999, pages 398-412, XP000911819 ISBN: 3-540-66347-9 abstract page 402 - page 404	1-8
A	EP 1 109 350 A (SAGEM) 20 June 2001 (2001-06-20) page 3, paragraph 24 - page 4, paragraph 30	1-8

Form PCT/ISA/210 (continuation of second sheet) (January 2004)

IPR2022-00412
Apple EX1053 Page 853

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IB2004/000738

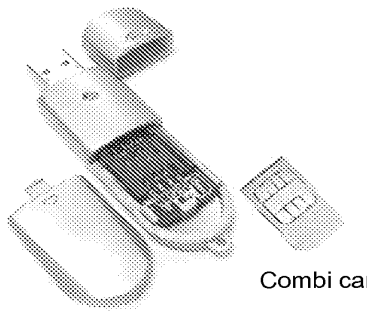
Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO 0131422 A	03-05-2001	AU	773982 B2	10-06-2004
		AU	2301401 A	08-05-2001
		CA	2388971 A1	03-05-2001
		CN	1413398 T	23-04-2003
		EA	3874 B1	30-10-2003
		EP	1226681 A2	31-07-2002
		JP	2003513490 T	08-04-2003
		WO	0131422 A2	03-05-2001
		ZA	200202798 A	10-07-2003
EP 1109350 A	20-06-2001	FR	2802741 A1	22-06-2001
		EP	1109350 A1	20-06-2001

IPR2022-00412
Apple EX1053 Page 854

advanced card systems ltd

ACR38CT

Technical Specification



Combi card

ACR38CT Contactless SIMTracker

Advanced Card Systems Ltd.
Unit 2910 - 2913, 29/F, The Center
99 Queen's Road Central, Hong Kong

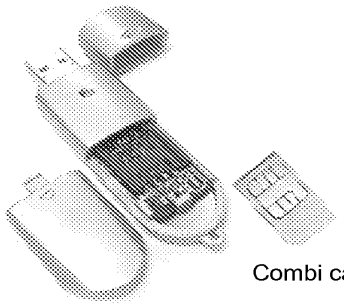
Tel: 852-2796 7873
Website: www.acs.com.hk

Fax: 852-2796 1286
E-mail: info@acs.com.hk

IPR2022-00412
Apple EX1053 Page 855

ACR38CT Contactless SIMTracker

1.0 Introduction



Combi card

Because of the growth of methods of working (remote office, home office...) and risk of hacking, it is the time to properly secure access to PCs, desktops, Intranet & Extranet networks and physical access control. ACR38CT offers both solutions based on **combi smart card** (contactless and contact card) for logical and physical access control.

The ACR38CT contactless SIMtracker is extension of ACR38T SIMTracker II. It has full ACR38T functionalities with contactless value-added feature.

i) Serves as a plug-in (SIM-sized) card reader:
It is an extremely compact USB full speed device fully compatible with the ACR38 smart card reader and is designed to access SIM sized smart cards (Plug-in card). With a size of only 82.5 mm x 21.3 mm x 9.4 mm, the ACR38CT is highly suitable for portable applications, as it plugs into the USB port and requires no additional cable or wiring. It also fulfils the GSM 11.11 specification. It is designed for PC environment, ultimate smart card peripheral for a PC.

ii) Serves as a contactless card:
While the ACR38CT serves as a contactless card, the **antenna coil** enables the contactless part of the combi card to work as a contactless card to communicate to contactless readers.

ACR38CT is a good quality, yet reliable and effective smart card to PC interfaces with designs focusing convenient use and harmony with other PC peripherals in shape and color. It also provides the solution where the security of a smart card is required. It can be used as logical and physical access control. It is ideal for electronic commerce, home banking or e-purse facilities, secure computer access, transportation, physical access control and GSM application tool..

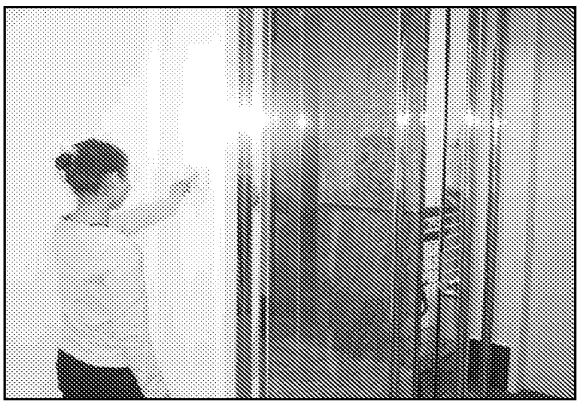
2.0 Features

- **USB full speed** interface to PC with simple command structure
- Support Plug-in SIM-sized card
- Read and write all microprocessor cards with T= or T=1 protocols
- Supports SLE 4418/28/32/42 memory cards
- Supports most common memory-based smart cards, including **I2C bus protocol cards** (from 1k bits up to 1024k bits) and secure memory cards (**Atmel AT88SC153** and **AT88SC1608**)
- Support **1.8V. 3V** and **5V** MCU cards
- Support GSM 11.11 specification
- Requires no additional cable
- Short Circuit Protection
- ISO 7816-1/2/3, PC/SC, CE, FCC
- ISO7816-1/2/3 compatible smart card interface
- Support PPS (Protocol and Parameters Selection) with 1743 – 305200 bps in reading and writing smart cards

Advanced Card Systems Ltd.
Unit 2910, 29/F, The Center, 99 Queen's Road Central, Hong Kong
Tel: (852) 2796 7873 Fax: (852) 2796 1286
Website: www.acs.com.hk E-mail: info@acs.com.hk

3.0 Typical Applications

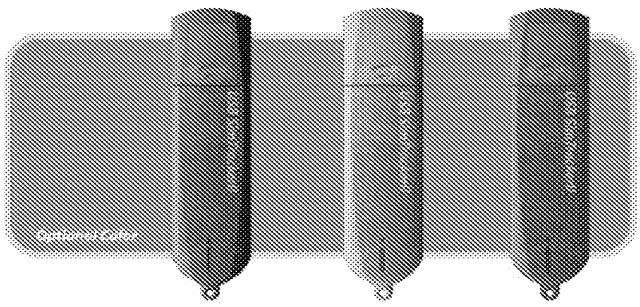
- Home Banking and Home Shopping
- Electronic Commerce
- Checking the balance of account of re-loading an electronic purses
- Network access control
- S/W locking
- Digital signature
- Loyalty and promotions
- Stored value
- Identification
- Ticketing
- Parking and toll collection
- Online gaming
- Transportation
- Physical access control



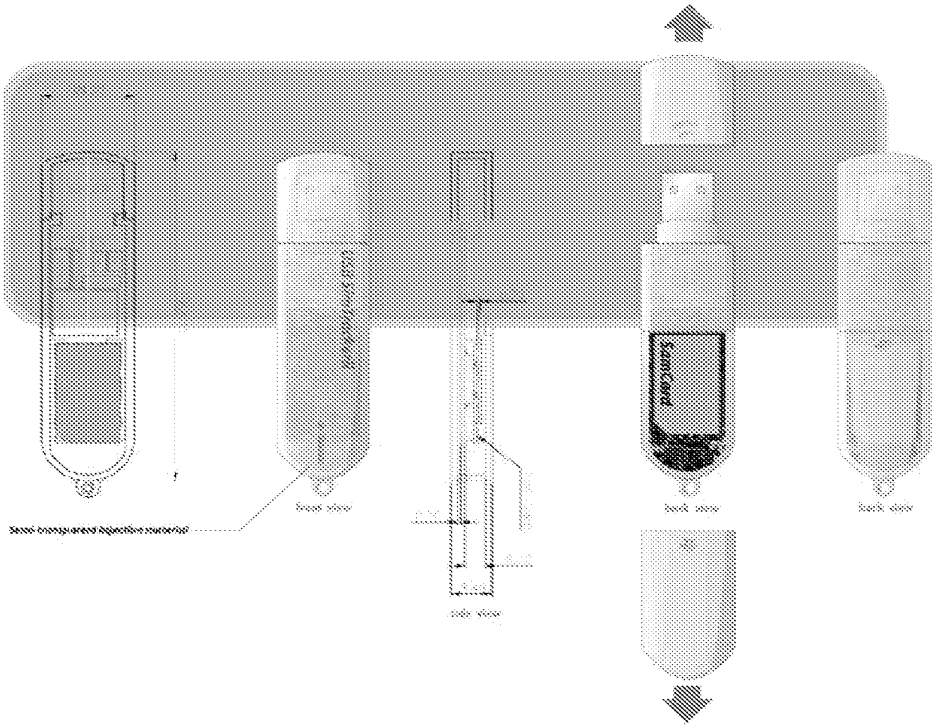
Serves as a contactless card - Physical access control

4.0 OEM possibility

The ACR38CT contactless SIMtracker is available for custom branding for promotion purposes. OEM enquiry is welcome. Casing color can be easily defined, and your own logo or design can be printed. We can also make other adaptations according to your requirements.



5.0 Technical Specification



Universal Serial Bus Interface	
Type	USB full speed, four lines: +5V, GND, D+ and D-
Power source	From USB
Smart Card Interface	
Standard	ISO 7816 1/2/3, T=0 and T=1
Supply current	max. 50mA
Smart card read / write speed	1743 – 305200 bps
Short circuit protection	+5V / GND on all pins
	The presence of the smart card power supply voltage is indicated through a green LED on the reader
CLK frequency	4 MHz
Card connector	sliding contacts (8 contacts)
Card insertion cycles	min. 100,000
Case	
Dimensions	82.5mm (L) x 21.3mm (B) x 9.4mm (H)
Standard color	Silver/golden
Weight	0.16 kg
Operating Conditions	
Temperature	0 - 50° C
Humidity	40% - 80%
Standard/Certifications	
EMV Level 1, ISO7816-1/2/3, PC/SC, CE, FCC	
OS	
Windows 98, ME, 2K, XP	

Advanced Card Systems Ltd.
Unit 2910 – 2913, 29/F, The Center
99 Queen's Road Central, Hong Kong
Tel: (852) 2796 7873
Website: www.acs.com.hk
Fax: (852) 2796 1286
E-mail: info@acs.com.hk

Advanced Card Systems Ltd.

ACR38DT DualKey

TECHNICAL SPECIFICATIONS

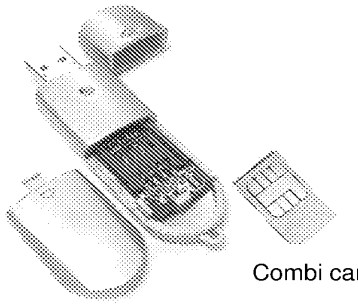
Version 1.3 09-2004

Advanced Card Systems Ltd.
Unit 2910-2913, 29/F, The Center,
99 Queen's Road Central, Hong Kong

Tel: +852 2796 7873 Fax: +852 2796 1286
Website: www.acs.com.hk Email: info@acs.com.hk

ACR38DT DualKey

1.0 Introduction



Combi card

Due to the rising demand of e-working methods (remote office, home office...) and snowballing hacking likeliness, it is the time to properly secure access to PCs, desktops, Intranet & Extranet networks and physical access control. ACR38DT offers both solutions based on SIM-sized **combi smart card** (contactless and contact card) for logical and physical access control.

The ACR38DT Contactless/Contact DualKey is an extension of ACR38T SIMTracker II. It has full ACR38T functionalities with contactless value-added feature.

i) Serves as a plug-in (SIM-sized) card reader:
It is an extremely compact USB full speed device completely compatible with the ACR38 smart card reader and is designed to access SIM-sized smart cards (Plug-in card). With a size of only 82.5 mm x 21.3 mm x 9.4 mm, the ACR38DT is highly suitable for portable applications, as it plugs into the USB port and requires no additional cable or wiring. It also fulfils the GSM 11.11 specification. It is designed for PC environment, ultimate smart card peripheral for a PC.

ii) Serves as a contactless card:
While the ACR38DT serves as a contactless card, the embedded antenna coil enables the contactless part of the SIM-sized combi card to work as a contactless card to communicate with contactless readers.

ACR38DT DualKey is a good quality, reliable and effective reader with designs focusing on convenient use and harmony with other PC peripherals in terms of shapes and colors. It is ideal for electronic commerce, physical access control, home banking or e-purse facilities, secure computer access, transportation and GSM application tool.

2.0 Features

- **USB full speed** interface to PC with simple command structure
- Support Plug-in SIM-sized card
- Read and write all microprocessor cards with T=0 or T=1 protocol
- Support SLE 4418/28/32/42 memory cards
- Support the most common memory-based smart cards, including **I2C bus protocol cards** (from 1k bits up to 1024k bits) and secure memory cards (**Atmel AT88SC153** and **AT88SC1608**)
- Support **1.8V. 3V** and **5V** MCU cards
- Support GSM 11.11 specification
- Require no additional cable
- Short Circuit Protection
- ISO 7816-1/2/3, PC/SC, CE, FCC
- ISO7816-1/2/3 compatible smart card interface
- Embedded antenna coil
- Full functionality with SIM-sized Combi card in contact and contactless interface
- Support PPS (Protocol and Parameters Selection) with 1743 – 307200 bps in reading and writing smart cards
- A patented technology combines physical and logical access control capabilities

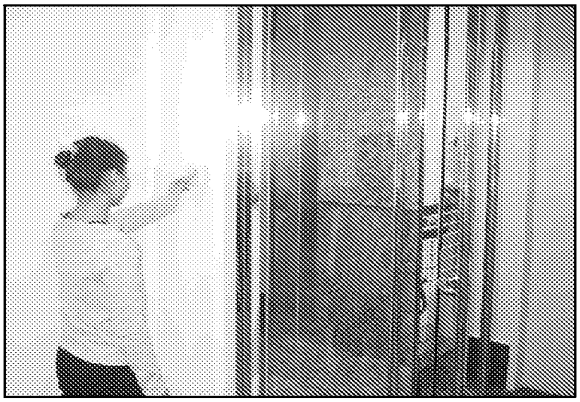
Advanced Card Systems Ltd.
Unit 2910-2913, 29/F, The Center,
99 Queen's Road Central, Hong Kong
Tel: +852 2796 7873 Fax: +852 2796 1286
Website: www.acs.com.hk Email: info@acs.com.hk

© Advanced Card Systems Ltd.

IPR2022-00412
Apple EX1053 Page 860

3.0 Typical Applications

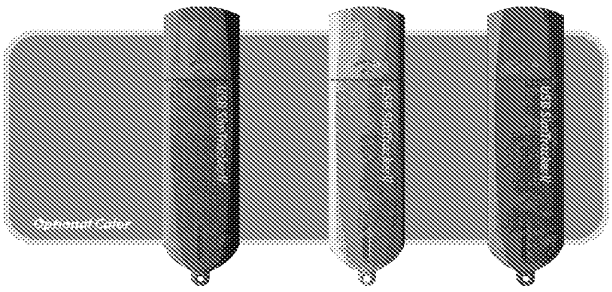
- Home Banking
- E-commerce
- Network access control
- Digital signature
- Identification
- Ticketing
- Parking and toll collection
- Online gaming
- Transportation
- Physical access control



Serves as a contactless card - Physical access control

4.0 OEM possibility

The ACR38DT DualKey is available for custom branding for promotion purposes. OEM enquiry is welcome. Casing color can be easily defined, and your own logo or design can be printed. We can also make other adaptations according to your requirements.

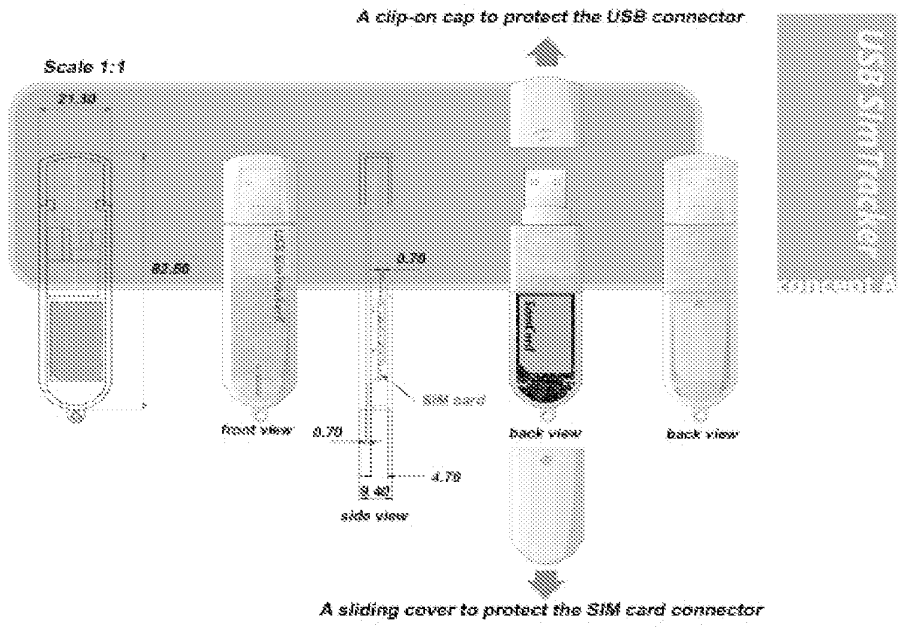


Advanced Card Systems Ltd.
Unit 2910-2913, 29/F, The Center,
99 Queen's Road Central, Hong Kong
Tel: +852 2796 7873 Fax: +852 2796 1286
Website: www.acs.com.hk Email: info@acs.com.hk

© Advanced Card Systems Ltd.

IPR2022-00412
Apple EX1053 Page 861

5.0 Technical Specification



Universal Serial Bus Interface	
Type	USB full speed, four lines: +5V, GND, D+ and D-
Power source	From USB
Smart Card Interface	
Standard	ISO 7816 1/2/3, T=0 and T=1
Supply current	max. 50mA
Smart card read / write speed	1743 – 307200 bps
Short circuit protection	+5V / GND on all pins
	The presence of the smart card power supply voltage is indicated through a green LED on the reader
CLK frequency	4 MHz
Card connector	sliding contacts (6 contacts)
Card insertion cycles	min. 100,000
Case	
Dimensions	82.5mm (L) x 21.3mm (B) x 9.4mm (H)
Standard color	Silver/golden
Weight	0.16 kg
Operating Conditions	
Temperature	0 - 50° C
Humidity	40% - 80%
Standard/Certifications	
ISO7816-1/2/3, PC/SC, CE, FCC	
OS	
Windows 98, ME, 2K, XP	

Advanced Card Systems Ltd.
Unit 2910-2913, 29/F, The Center,
99 Queen's Road Central, Hong Kong
Tel: +852 2796 7873
Website: www.acs.com.hk
Fax: +852 2796 1286
Email: info@acs.com.hk

© Advanced Card Systems Ltd.

IPR2022-00412
Apple EX1053 Page 862

DS9490R/DS9490B

USB to 1-Wire/iButton Adapter

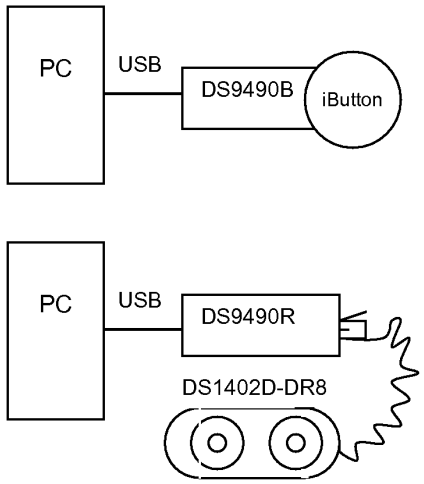
FEATURES

- High-Speed 12Mbps Universal Serial Bus (USB) Interface
- Supports Standard and Overdrive 1-Wire® Communication
- Slew-Rate-Controlled 1-Wire Timing and Active Pullup for Improved 1-Wire Network Performance
- DS9490R has an RJ11 Interface for Standard Connectivity Accessories such as the DS1402D-DR8
- DS9490B has an iButton® Interface and Retains a Fixed iButton
- Built-In Custom DS2401 Identification Chip
- Reads all 1-Wire and iButton Devices. Writes All Except EPROM 1-Wire/iButton Devices

APPLICATIONS

- Software Authorization—Protection against software piracy by tying software operation to the presence of iButton hardware.
- iButton Initialization and Download—Loggers like the Thermochron® can be missioned and downloaded. Monetary iButtons can be refilled with money.
- Demonstration—Demonstrate the features of iButtons or 1-Wire chips on personal computers.
- Development—Aid development of 1-Wire applications by providing a PC interface to verify device contents and state.

TYPICAL OPERATING CIRCUIT



ORDERING INFORMATION

PART	DESCRIPTION
DS9490B	USB Single F5 iButton Holder with Protective Cap
DS9490R	USB to 1-Wire RJ11

PACKAGING/SHIPPING INFORMATION

The part is shipped individually in an anti-static bag.

DESCRIPTION

The DS9490B is a USB bridge and holder for a single F5-size iButton. The iButton is securely held behind a latched door. The DS9490R is a USB bridge with 1-Wire RJ11 interface to accommodate 1-Wire receptacles and networks. The DS1402D-DR8 (Blue Dot™) can readily be used in conjunction with the DS9490R to create an iButton PC reader. Both adapters are based on the DS2490 USB to 1-Wire bridge chip.

PC software drivers for Windows® 98, Windows 2000, Windows ME, and Windows XP can be found on the iButton website under software support at: http://www.ibutton.com/software/tmex/index.html

1-Wire, iButton, and Thermochron are registered trademarks of Dallas Semiconductor.
Blue Dot is a trademark of Dallas Semiconductor.
Windows is a registered trademark of Microsoft Corp.

IPR2022-00412
Apple EX1053 Page 863

Figure 1. DS9490R

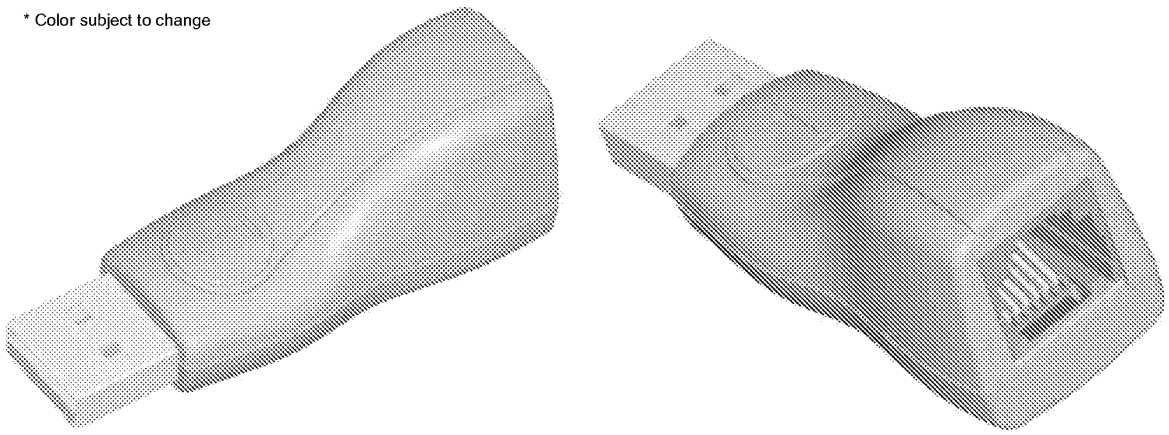
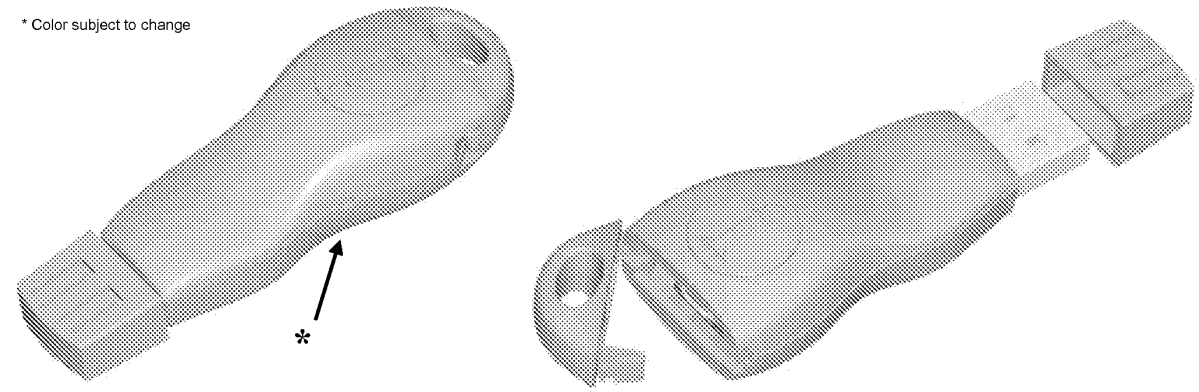


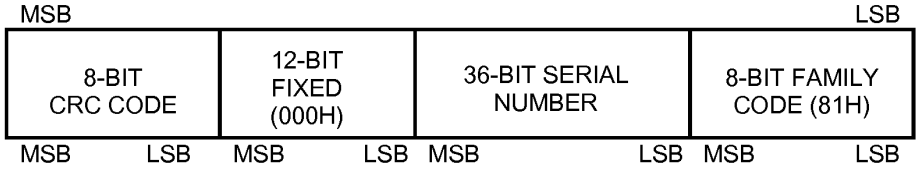
Figure 2. DS9490B



***Note:** To eject an iButton, insert a straightened paper clip into the side access hole of the DS9490B. Push the paper clip in the direction of the iButton. A different iButton can then be inserted. The data contact faces down and away from the embossed 'i'. Before inserting the paper clip disconnect the DS9490B from the USB bus.

Each USB bridge contains a unique built-in identification chip. The identification chip is a custom DS2401 that is a 64-bit ID number (see Figure 3).

Figure 3. DS2401 ID CHIP 64-BIT LASERED ROM



IPR2022-00412
Apple EX1053 Page 864

PIN CONFIGURATION

Figure 4. 1-WIRE RJ11 SOCKET FOR DS9490R

PIN	SIGNAL NAME	DESCRIPTION
1	V_{DD}	5VDC Output
2	GND	Power Ground
3	OW	1-Wire Data
4	GND_OW	1-Wire Return
5, 6	N.C.	No Connection
6	N.C.	No Connection

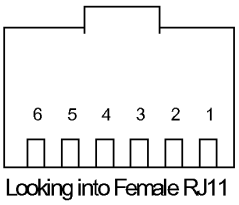
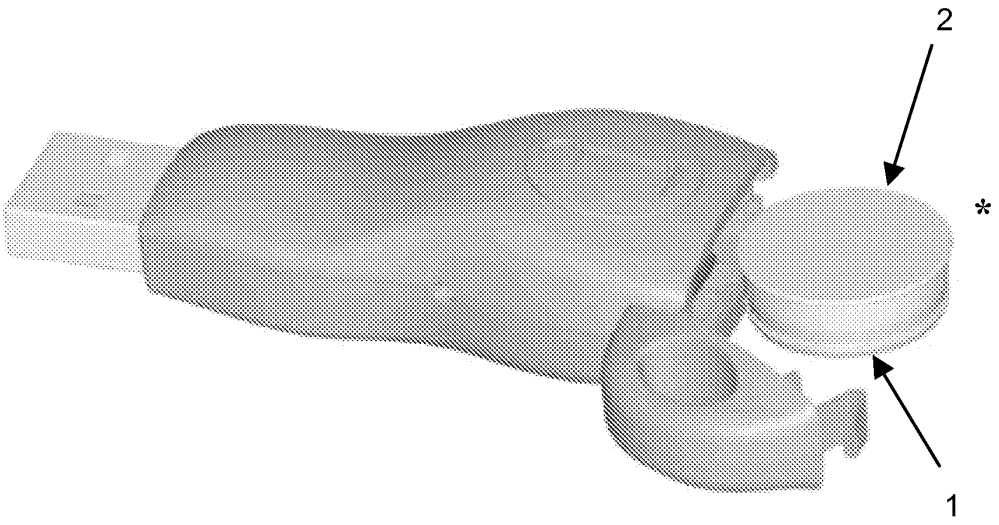


Figure 5. iBUTTON SOCKET FOR DS9490B

PIN	SIGNAL NAME	DESCRIPTION
1	OW	1-Wire Data
2	GND_OW	1-Wire Return



***Note:** The data contact faces down and away from the embossed 'i'. Once the iButton is inserted in the enclosure, snap the end cap over it. The end cap is removed by depressing the release tab, swinging it fully open, and sliding out the hinge.

IPR2022-00412
Apple EX1053 Page 865

MECHANICAL DIMENSIONS

All dimensions are in millimeters.

Figure 6. DS9490R

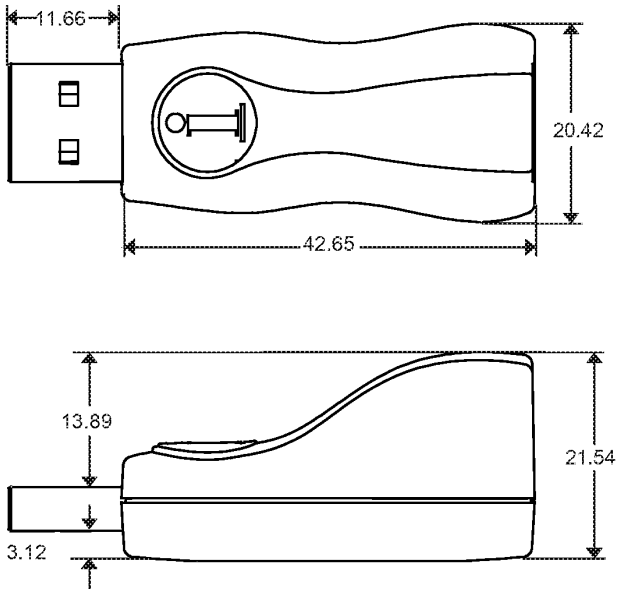
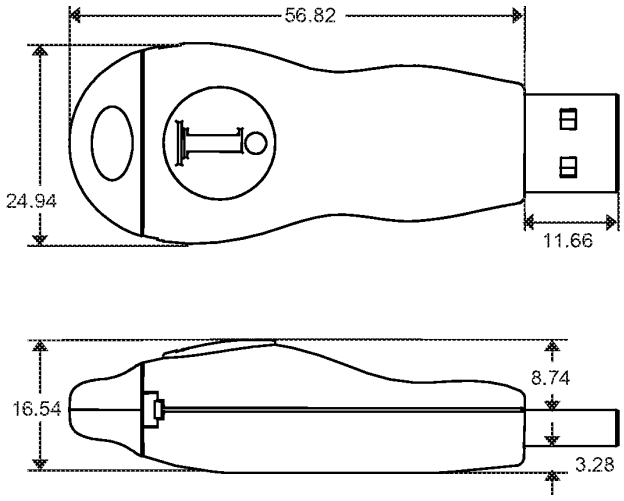


Figure 7. DS9490B



ENVIRONMENTAL REQUIREMENTS

CONDITION	PARAMETER	VALUE
Storage	Temperature	-10°C to +85°C
Storage	Relative humidity, noncondensing	95%
Storage	Duration	1yr (max) at 95%RH and +85°C
Operating	Temperature	0°C to +70°C
Operating	Relative humidity, noncondensing	80%

IPR2022-00412
Apple EX1053 Page 866

ELECTRICAL CHARACTERISTICS

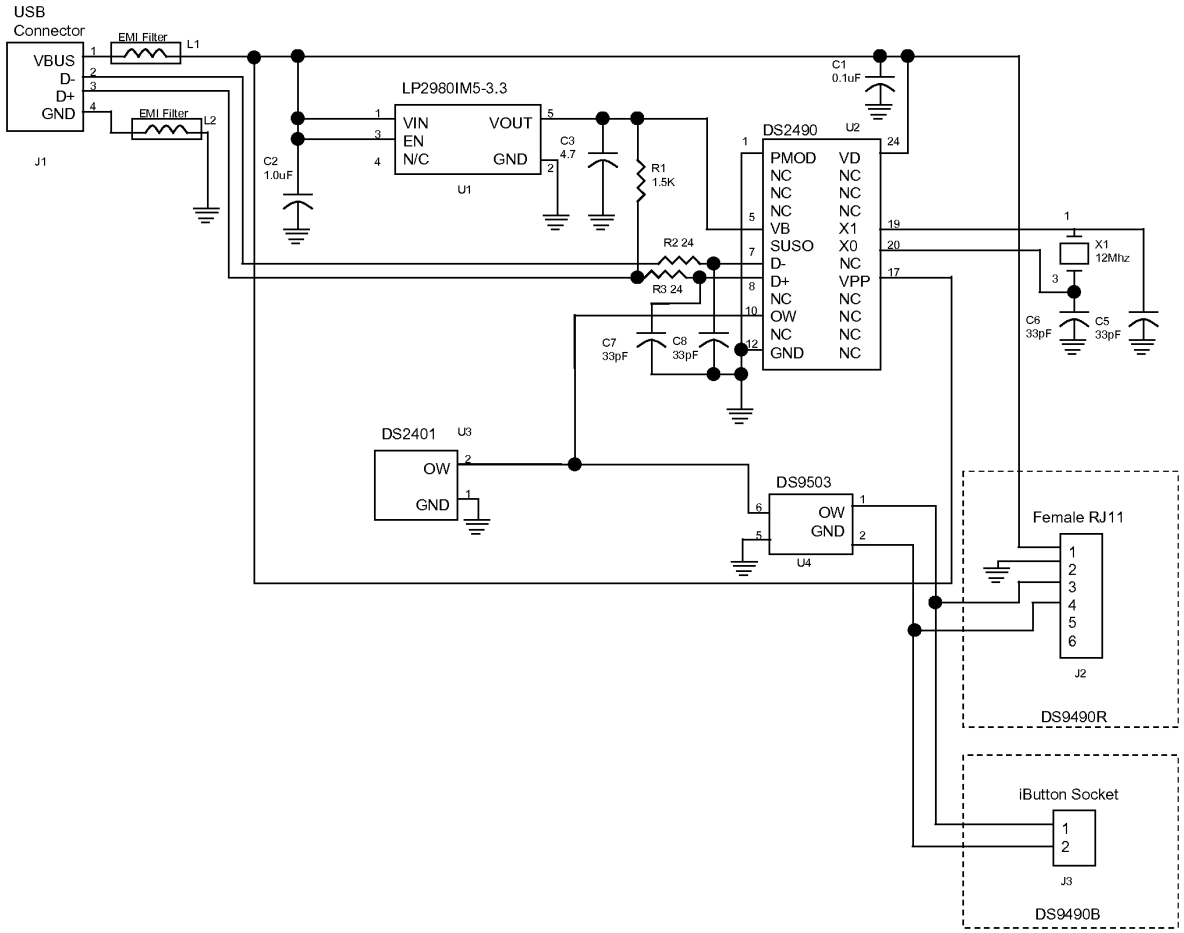
PARAMETER	SPECIFICATION
USB I/F	As defined in Chapter 7 of the USB Specification*
1-Wire I/F	See the DS2490 data sheet**

The DS9490R and DS9490B consume 58mA in USB active mode and 0.5mA in suspend mode*. The DS9490R has the V_{BUS} power and ground available on the RJ11 connector. In active mode the current available to an externally powered fixture is 42mA* (100mA to 58mA); however it is recommended that no more than 25mA be used. Note that in suspend mode there is zero current available to an external circuit. An external circuit cannot detect when the module is in suspend or active mode. Consequently, when in suspend mode, the DS9490R module with external circuit combination is in violation of the USB power specification. Application developers should be aware of this when using this module in conjunction with an externally powered circuit on power restricted platforms such as laptops.

*Guaranteed by design, not production tested.

**Tested at DS2490 component level.

Figure 8. FUNCTIONAL DIAGRAM



IPR2022-00412
Apple EX1053 Page 867