(12) STANDARD PATENT (11) Application No. AU 2001239626 B2
(19) AUSTRALIAN PATENT OFFICE

(54) Title
Key and lock device

(51)7 International Patent Classification(s)
E05B 049/00

(21) Application No: **2001239626** (22) Date of Filing: **2001.03.09**

(87) WIPO No: **WO01/66887**

(30) Priority Data

(31) Number	(32) Date	(33) Country
0000794	**2000.03.10**	**SE**

(43) Publication Date: **2001.09.17**
(43) Publication Journal Date: **2001.11.29**
(44) Accepted Journal Date: **2004.12.23**

(71) Applicant(s)
Assa Abloy AB

(72) Inventor(s)
Lefebvre, Arnaud; Kikebusch, Bernd; Kruhn, Jurgen; Chanel, Christophe; Brennecke, Gudrun; Sivonen, Hannu; Magnusson, Bjorn; Norberg, Rolf; Liden, Inge

(74) Agent / Attorney
FB Rice & Co, 605 Darling Street, Balmain, NSW, 2041

(56) Related Art
EP0410024
US48887292
US5552777
EP0239342

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 September 2001 (13.09.2001)

PCT

(10) International Publication Number
WO 01/66887 A1

(51) International Patent Classification⁷: E05B 49/00

(21) International Application Number: PCT/SE01/00500

(22) International Filing Date: 9 March 2001 (09.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0000794-8 10 March 2000 (10.03.2000) SE

(71) Applicant: **ASSA ABLOY AB** [SE/SE]; Box 70340, S-107 23 Stockholm (SE).

(72) Inventors: **LIDÉN, Inge**; Friluftsvägen 13, S-633 59 Eskilstuna (SE). **NORBERG, Rolf**; Illervägen 29A, S-187 35 Täby (SE). **MAGNUSSON, Björn**; Viktoriavägen 1, S-147 31 Tumba (SE). **SIVONEN, Hannu**; Marjovaarantie 40, FIN-82815 Marjovaara (FI). **BRENNECKE, Gudrun**; Harlinger Strasse 1, 14199 Berlin (DE). **CHANEL, Christophe**; Wilmerdorferstrasse 125, 10672 Berlin (DE). **KRÜHN, Jürgen**; Baseler Strasse 162a, 12205 Berlin (DE). **KIKEBUSCH, Bernd**; Windsteiner Weg 53a, 14165 Berlin (DE). **LEFEBVRE, Arnaud**; 92, Avenue Pasteur, F-10000 Troyes (FR).

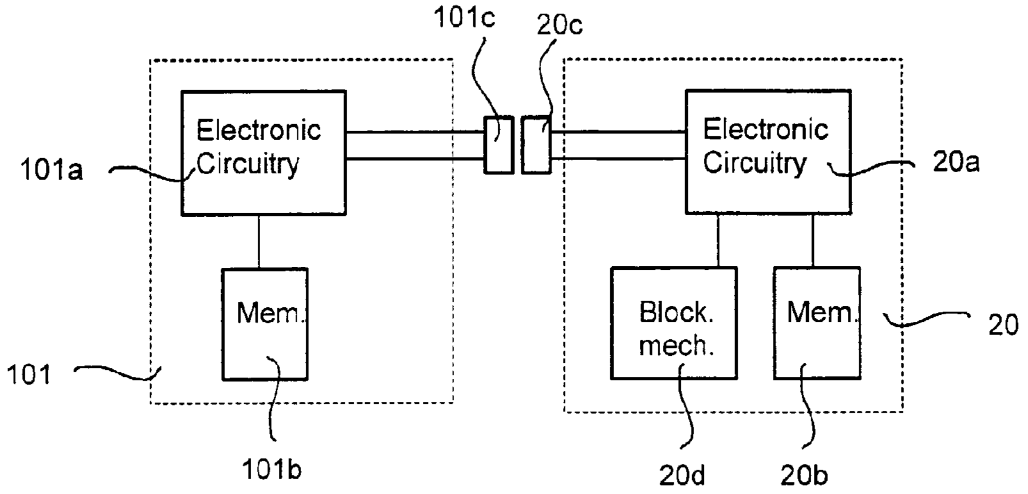
(74) Agents: **ESTREEN, Lars** et al.; Kransell & Wennborg AB, Box 27834, S-115 93 Stockholm (SE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), 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, SK (utility model), 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 patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,

[Continued on next page]

(54) Title: KEY AND LOCK DEVICE



(57) Abstract: A key and lock device comprises a key (101) and a stand-alone lock (20). The key has an electronic circuitry (101a) with a first memory (101b), and a first contact (101c). The lock (20) has an electronic circuitry (20a) with a second memory means (20b), and a second contact means (20c) arranged to co-operate with the first contact means (101c). Also, there is a blocking mechanism (20d) adapted to block operation of the lock unless an authorised key is inserted in the lock. The memory of the key stores a public identification item of the key identifying a group of keys having identical mechanical codes. In the memory of the lock, there is provided a list of the public and secret identification items of authorised keys and a list of the public identification item of non-authorised keys. A key is authorised if the public and secret identification items are present in the list of authorised keys and the public identification item thereof is absent in the list of non-authorised keys. This provides for an easy and flexible way of authorising key and lock devices and adding new keys to a system.

WO 01/66887 A1

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:

— *with international search report*

2001239626 30 Sep 2004

AUSTRALIA

Patents Act 1990

ASSA ABLOY AB

COMPLETE SPECIFICATION
STANDARD PATENT

Invention Title:

Key and lock device

The following statement is a full description of this invention including the best method of performing it known to us:-

2001239626 30 Sep 2004

KEY AND LOCK DEVICE

FIELD OF INVENTION

The present invention relates generally to key and lock devices, and more specifically to electromechanical key and lock devices and lock systems comprising such devices.

BACKGROUND

It is previously known a variety of lock devices that use electronic devices for increasing the security of the lock and for providing effective administration, management, and control of keys and personnel. However, these devices have had the inherent drawback of either being wired with accompanying high installation costs or stand alone devices requiring significant individual efforts to change or extend the system with keys and/or locks.

Another drawback of prior art lock systems is that they are difficult to create and adapt to the specific requirements of a customer.

The US patent document US 4,887,292 (Barrett et al.) discloses an electronic lock system provided with a "lockout list" that identifies keys that are to be prevented from opening system locks. This system is adapted to be used with real estate lockboxes used in the real estate industry to contain the keys of houses listed for sale. The inflexibility of the disclosed system results in it not addressing the above mentioned problems of prior art key and lock systems.

Any discussion of documents, acts, materials, devices, articles or the like which has been included in the present specification is solely for the purpose of providing a context for the present invention. It is not to be taken as an admission that any or all of these matters form part of the prior art base or were common general knowledge in the field relevant to the present invention as it existed before the priority date of each claim of this application.

Throughout this specification the word "comprise", or variations such as "comprises" or "comprising", will be understood to imply the inclusion of a stated element, integer or step, or group of elements, integers or steps, but not the exclusion of any other element, integer or step, or group of elements, integers or steps.

SUMMARY OF THE INVENTION

According to a first aspect, the present invention provides an electromechanical key and lock device, comprising:

- a key having a mechanical code and a key electronic circuitry comprising
  - a lock memory adapted for storing a public identification item of said key, and
  - a key contact; and
- a stand-alone lock having a lock electronic circuitry comprising
  - a lock memory,
  - a lock contact arranged to co-operate with said key contact, and
  - a blocking mechanism adapted to block operation of said lock unless an authorised key is inserted in the lock;

characterized in that

- said public identification item of said key comprises a group identification item identifying a group of keys having identical mechanical codes, and
- said lock memory is adapted for storing
  - a list of said public identification item and a secret identification item of authorised keys, and
  - a list of said public identification item of non-authorised keys,
- wherein a key is authorised if said public and secret identification items thereof are present in the list of authorised keys and said public identification item thereof is absent in the list of non-authorised keys.

According to a second aspect, the present invention provides a lock system, comprising a key and lock device in accordance with the first aspect of the invention.

According to a third aspect, the present invention provides a method of updating authorisation information of a lock system in accordance with the second aspect of the invention, characterized by the step of updating said information in said lock memory of said lock device.

Embodiments of the present invention may provide for easy adding or deleting of authorisation of access to the operation of a lock by the key.

Other embodiments of the present invention may provide an electromechanical key and lock device of the kind initially mentioned wherein the distribution and assignment of keys are more secure than in known lock systems.

Further embodiments of the present invention may provide a lock system with a high level of key control and wherein no keys can be added without the knowledge of the system owner.

Still further embodiments of the present invention may provide a lock system with a high level of authorisation control.

Other embodiments of the present invention may provide a lock system that is easy to create and service.

Yet other embodiments of the present invention may provide a key and lock device wherein the assignment of keys is facilitated.

The invention is based on the realisation that certain information elements or items of an electronic key code will provide for a simple and yet secure distribution and assignment of keys in a master key system.

By providing a group concept together with lists indicating authorised and non-authorised devices easy adding and deleting of keys and locks is made possible while a high level of security is maintained. In a non-wired system, the group concept makes it possible to add new keys to the system without having to access or alter existing locks.

BRIEF DESCRIPTION OF DRAWINGS

The invention is now described, by way of example, with reference to the accompanying drawings, in which:

Fig. 1 is an overall view of a lock system according to the invention;

Fig. 2 is a block diagram of a key and lock device according to the invention;

Fig. 3 is a diagram showing the group concept used with the invention;

Figs. 4a and 4b are diagrams showing information elements in a key and a lock, respectively, according to the invention; and

Fig. 5 is a diagram showing an example of distribution of locks in an office building.

DETAILED DESCRIPTION OF THE INVENTION

In the following, a detailed description of preferred embodiments of the invention will be described.

Lock system and Tools

A lock system comprising lock devices according to the invention will now be described with reference to figure 1, which shows the distribution of hardware and software tools among different hierarchical levels of a lock system, namely customer 100, distributor 200 and manufacturer 300. The manufacturer, distributors and customers constitute the members of the overall lock system.

Each element, i.e., key, lock etc., in the system belongs to one and only one master key system. This is to maintain the high security levels required of today's lock systems.

Software

At each level there is software installed. There are three different kinds of software, one for each of the three levels: Manufacturer software (M-software), Distributor software (D-software) and Customer software (C-software).

Each installed software maintains a database comprising information, such as encryption keys etc. In case the communication encryption keys must be changed, the manufacturer sends the new keys encrypted with the current communication encryption key.

User keys

In the customer system 100, there are several user keys 101 adapted for use with a number of locks 20.

Programming and authorisation key

There is at least one special programming and authorisation key (C-key) 102 for a customer system. A C-key can be a normal looking key, but with special features. It includes, like a normal user key, a simple user interface, either a small display or a buzzer.

There is a defined routine and sequence to replace a lost C-key. This routine leads back to the factory for authorisation.

Customer programming box

At the customer, there is a programming box 106 adapted for connection to a computer (PC) 104 via e.g. a serial interface. This programming box comprises a static reader 107 and is used for programming keys and locks in the customer system. A static reader is a key reader without a blocking mechanism and thus comprises electronic circuits etc. for reading and programming a key.

Optionally, the programming box can be provided with an internal power source, thus also functioning as a stand alone box operating disconnected from the computer 104.

Although a customer programming box is shown in the figure, this box can be omitted in very small lock systems.

Customer software

The customer has access to a personal computer 104 running customer administration software (C-software) with open system information only. Thus, the C-software keeps track of which keys are authorised in which locks in the lock system in question. It also contains information regarding secret identities of all keys of a system.

Authorisation key for the distributor

There is an authorisation key (D-key) 202 for the distributor of the lock system, who can be e.g. a locksmith. The function of this key is equivalent of the C-key. However, a D-key has special authorisation data for the particular software with which it will be used. A D-key is also used as a secure communication bridge for all distributor level programming.

Distributor programming box

At the distributor, there is a programming box 206 adapted for connection to a computer (PC) 204 via e.g. a serial interface, like a RS232C interface. This programming box can be identical to the one described in connection with the customer system 100.

Distributor software

The distributor has special computer software (D-software) for a personal computer 204. The D-software includes an open part for display of open system information and for design of changes etc. It also includes a secret part including authorisation codes and secret keywords used in the system. The D-software also supports encrypted communication to manufacturer lock system computer 304 through e.g. a modem connection 208.

The D-software stores secret identities of keys, but not in plain text but in an encrypted format. However, the encryption keys are not stored with the D-software but is present in the D-key. Thus, the D-key is needed when the encrypted information is to be read.

The distributor software may use as a module a key/lock register, which constitutes the customer system. In that way, the distributor can work transparently as if the distributor and customer software were one system. This is necessary for the distributor if he is going to be closely involved with servicing the customer system.

Manufacturer key

There is an authorisation key (M-key) 302 with a function similar to the D-key, but with authorisation to M-software including all master key systems delivered by the manufacturer in question.

Manufacturer programming box

This is a programming box 306 similar to the distributor programming box.

Manufacturer software

The manufacturer has access to a personal computer 304 running software (M-software) with full authorisation for all operations.

The tools used create a flexible environment, which can be configured in a way to fit the market conditions. Authorisation can be limited or extended at the different levels. However, the manufacturer can always do everything that can be done. The distributor can never store secret codes himself and the customer can normally not create a new or extended system himself. The manufacturer can hereby control the level of authorisation for the distributor and the distributor can control the system maintenance.

The above mentioned tools together determine the possible operations of the different parts. In practice, the system can operate in many different structures and set-ups. It all depends on to whom the different tools are distributed. This provides a flexible system, which can be adapted for a wide range of applications.

KEY AND LOCK ELECTRONICS

In the following, a description of the key and lock electronics will be given with reference to figure 2, which is a schematic block diagram of a key and a lock.

The key, generally designated 101 comprises an electronic circuitry 101a having a microprocessor, timer circuits etc. for executing the normal operations of a microprocessor arrangement. Specifically, a memory circuit 101b has been shown electrically connected to the electronic circuitry. This memory circuit is used for storing information regarding the key, as will be explained below.

A contact 101c placed on the exterior of the key 101 is also shown electrically connected to the circuitry 101a.

The lock, generally designated 20, comprises an electronic circuitry 20a having a microprocessor, timer circuits etc. for executing the normal operations of a microprocessor arrangement. This circuitry 20a is similar to the one 101a located in the key. This is an advantage in that large-scale production reduces manufacturing costs.

A memory circuit 20b is shown electrically connected to the electronic circuitry 20a. This memory circuit is used for storing information regarding the lock and authorised keys, as will be explained below.

A contact 20c is located in the lock 20 and is shown electrically connected to the circuitry 20a. This lock contact is arranged to co-operate with the key contact 101a in order to establish electric connection between the key electronics and the lock electronics.

There is also an electrically controlled blocking mechanism 20d in the lock 20. This mechanism is controlled by means of driving circuitry (not shown) and opens the lock as a result of identification of an authorised key in the lock.

GROUP CONCEPT

The customer level 100 of the master key system described with reference to figure 1 can be divided into different groups and each user key 101 belongs to one and only one group. However, the groups can be defined according to several different rules, which will be described in the following.

Standard solution

The standard solution is to have one key cut per individual door and one group per mechanical key cut. This solution is used in prior art lock systems and thus does not require any modification of the thinking of developing a new MKS. This gives a very secure but somewhat inflexible solution.

Organisational solution

According to the organisational solution, one mechanical key-cut and one group is assigned to each "department" of the organisation using the MKS. Thus, in a typical company, the sales department, research and development department, security guards, production department 1, production department 2 etc. are each assigned to a specific group. This is illustrated in figure 3 showing the customer level of a MKS according to the invention.

The advantage of this solution is that less different mechanical key-cuts are required and that it gives flexibility in the set-up of the system.

One key-cut, many groups

According to this solution, few key-cuts are made. As an example, all individual user keys of one floor, several floors or even the entire company have the same key-cut. Further, all master keys have the same key-cut, sub-master keys level 1 have another, level 2 yet another etc.

Groups are then defined as in the organisational solution described with reference to figure 3.

This solution gives very few mechanical key-cuts, resulting is a very flexible master key system.

The described solutions may of course be varied depending on the special requirements of the system. As an example, some departments may be divided into several groups. Alternatively, several small departments may constitute one group. The way the group concept is used can also vary within an organisation. However, an important feature is that all keys in one group are mechanically identical, i.e., with identical key-cuts. The reason therefor will be described below.

INFORMATION ELEMENTS

All keys and locks have a unique electronic identity or code comprising several information elements controlling the functions of the keys and locks. The information elements of a key or a lock will now be described with reference to figure 4a and 4b, respectively.

The code is divided into different segments for the use of manufacturers, distributors, customers and individual key data's while a secret segment is provided for secret information and is always individual for the group.

All keys and locks have a unique electronic code or identity. Every lock code comprises the following parts:

- Manufacturer identification (M)
- Public Lock ID (PLID) comprising
  - Master Key System identification (MKS)
  - Function identification (F)
  - Group ID (GR)
  - Unique Identity (UID)
- DES key
- Secret Lock ID (SLID) comprising
  - Secret group ID (SGR)

Correspondingly, every key code comprises the following parts:

- Manufacturer identification (M)
- Public Key ID (PKID) comprising
  - Master Key System identification (MKS)
  - Function identification (F)
  - Group ID (GR)
  - Unique Identity (UID)
- DES key
- Secret Key ID (SKID) comprising
  - Secret group ID (SGR)

The basic elements will now be described in more detail.

M – Manufacturer

M identifies the manufacturer of the master key system. In the description and examples of the invention given below, this element is omitted as all keys and locks are assumed to have the same manufacturer.

MKS – Master Key System

MKS identifies the different Master Key Systems. A lock will accept a user key or a C-key only if they have the same MKS code. In the description and examples of the invention given below, this element is omitted as all keys and locks are assumed to belong to the same master key system.

F – Function

F identifies the role of the device; whether it is a lock, a user key, a C-key, D-key or M-key.

GR – GRoup

GR is an integer identifying the group. GR is unique in each MKS and starts at 1 with an increment of 1.

UID – Unique Identity

UID identifies the different users in a group. UID is unique in each GR, starts at 1 with an increment of 1.

DES

The DES comprises a randomly generated DES encryption key, the same in one MKS. The DES is in no way readable from the outside and is only used by the algorithms executed internally of the key and lock devices.

SGR – Secret GRoup

SGR is a randomly generated number that is the same for one GR.

AUTHORISATION TABLE

In every lock there is an authorisation table stored in electronic memory. The authorisation table determines which keys the lock in question accepts. The configuration and function will now be discussed.

The authorisation table is divided into two parts, a list of authorised keys (the A-list) and a list of non-authorised keys (the NA-list). A key is authorised only if it is listed in the A-list but not in the NA-list. The A-list comprises both the PKID and the SKID of authorised keys. However, the NA-list comprises only the PKID and not the SKID of non-authorised keys.

A key is listed by its group or its unique identity. In both cases, it is determined by the PKID, comprising the information elements GR-UID, see figure 4a. To specify the unique identity, the values of both GR and UID are provided. However, in the case a group is to be specified, UID is given the value "0", denoting no specific key, because the UID for individual keys can take the values "1", "2", "3" etc. As an example, a PKID of 2-0, i.e., GR=2 and UID=0, denotes the entire group 2 of the master key system in question.

It is thus possible to authorise all keys of one group in one lock by memorising UID=0 for the GR in question. With this solution, all keys of a group, whatever their UID, will be authorised to open the lock, provided they are not listed in the NA-list. This allows the making of a new key, with a new UID, working directly in the lock without one having to reprogram the lock.

As already stated, when a key is listed in the A-list, the secret key identity SKID is stored, too. The SKID is the same for all keys of one group and is used for security reasons. It is not possible to read the SKID from the keys or locks without having fulfilled special authentication procedures by means of a C-key, which will be discussed below.

If an entire group is authorised in the manner described above, it is possible to restrict the access of one or more keys of that group by including their PKID in the NA-list of the lock.

An example of organisational grouping and authorisation will now be given with reference to figure 5, wherein an office building including an R&D department and a sales department is schematically shown. The entire office belongs to master key system 1, i.e., MKS=1 for all keys and locks. There are all in all seven doors in the office, three belonging to the R&D department: R&D1, R&D2, and LAB, two belonging to the sales department: SALES1 and SALES2, and two common doors, MAIN and COMMON. There are four people working in the office, two in the R&D department, Researchers

1 and 2, and two in the sales department, Salespersons 1 and 2.

The master key system is divided into two electronically coded groups, GR=1 (R&D) and GR=2 (Sales), each group with two keys. The PKID of the keys are given in table 1 below:

TABLE 1a

Group	User	PKID (GR-UID)
1	Researcher 1	1-1
1	Researcher 2	1-2
2	Salesperson 1	2-1
2	Salesperson 2	2-2

The authorisation tables of the different doors are given in table 2

TABLE 2a

MAIN		R&D1		R&D2		LAB		COMMON		SALES1		SALES2	
A	NA	A	NA	A	NA	A	NA	A	NA	A	NA	A	NA
1-0		1-1		1-2		1-0		1-0		2-1		2-2	
2-0								2-0					

In common doors, entire groups are listed in the A-list and in private doors, only the specific keys admitted are listed in the A-list.

With this configuration, all four employees are admitted through the main door and to the common room. Only the researchers are admitted to the lab. To the four personal rooms, only the person working therein is admitted.

If one of the employees quits and is replaced by another, new keys must be issued and locks must be reprogrammed. Assume that Researcher 1 quits without returning his keys and is replaced by Researcher 3. The identities of the issued keys will now look like in table 1b:

TABLE 1b

Group	User	PKID (GR-UID)
1	Researcher 1	1-1
1	Researcher 2	1-2
1	Researcher 3	1-3
2	Salesperson 1	2-1
2	Salesperson 2	2-2

Access to the office must be denied to Researcher 1 and instead given to Researcher 3. The PKID of the key of Researcher 1 is therefore added to the NA-list of all locks where Researcher 1 was authorised. The PKID of the key of Researcher 3 must be added to his private room. The authorisation tables will then look like in table 2b:

TABLE 2b

MAIN		R&D1		R&D2		LAB		COMMON		SALES1		SALES2	
A	NA	A	NA	A	NA	A	NA	A	NA	A	NA	A	NA
1-0	**1-1**	1-1	**1-1**	1-2		1-0	**1-1**	1-0	**1-1**	2-1		2-2	
2-0		**1-3**						2-0					

Additions compared to table 2a are indicated by boldface.

It is thus very easy to make the necessary changes to the locks of the master key system.

It is appreciated that if there are identical entries in the A and the NA lists, both could be deleted to save memory.

The electronic coding can be supplemented by mechanical coding as well. In the present example, there can only be two mechanical cuttings, MC1 and MC2, as there are only two electronically coded groups and the mechanical coding must be the same within a group.

DEFINED OPERATIONS

In the following, an overview of the different operations in the system will be given. Initially, the original master key system is created and programmed by the manufacturer by means of the manufacturer software 304. This initial system includes one or more C-keys 102. A complete information on the created system is stored in the M-software 304.

There are a number of defined operations with their separate rules. The possible operations are listed in the following:

- Add Key
- Add C-key
- Replace Master C-key
- Delete Key
- Delete C-key
- Authorise Key
- Forbid Key
- Read Audit Trail
- Read Key List
- Test
- Read User Register
- Update User Register

Control commands for programming device

- Scan Programming Audit Trail
- Scan Test results
- Scan Key list from a lock
- Scan Audit trail list from a lock
- Identification of the lock
- Delete Task
- Delete Key List

- Delete Audit Trail
- Delete Programming Audit trail
- Delete all

Status data:

- Task activated in a C-key
- Task done for a lock
- Etc..

Some of these operations will now be discussed in detail.

Add Key Operation

A key is added to the number of authorised keys by adding its PKID and SKID to the A-list.

Delete Key Operation

To delete authorisation of a key, the PKID and the SKID of the key are deleted from the A-list. This is called the delete operation. From now on, the key is not authorised and to make it authorised, the add operation must once again be performed.

Forbid Key Operation

As already stated, when a key or a group is authorised in a lock, its SKID is also memorised in the A-list of the lock. It is possible to instruct a lock to copy the PKID to the NA-list and to leave the PKID and SKID in the A-list. In this case, the lock will not open to the key in question because a lock does not open to a key in the NA-list, even if it is in the A-list. This operation to copy the PKID to the A-list is called a forbid operation.

Reauthorize Key Operation

If a forbid operation has been performed on a key, it is possible to reauthorize the key without having its SKID, i.e., without access to the key itself. The only thing you have to do is to delete the PKID in the NA-list. This operation is called a reauthorization operation.

The combination of the forbid and reauthorize operations is useful when a key is to be reauthorize without having access to the key. It means that the PKID and the SKID of a key has to be entered in the A-list only once. Thereafter, forbid or reauthorization operations are performed.

Replace Key Operation

The replace operation enables manufacturing of a key that will tell all locks in which the key has been inserted that it is replacing a specific key. This operation can only be performed in locks in which the replaced key was authorised. The operation checks that the previous key is in the A-list and not in the NA-list. It then puts the PKID of the replaced key on the NA-list.

With this operation, reprogramming is effected automatically. This is particularly useful when a key has been lost.

Create Installer Key Operation

In the initial stages of the creation of a lock system, there is a need for a so-called "Installer Key". This is just a normal user key with authorisation in all locks of the system and which is used during installation. It must be excluded after use like any "lost" key.

C-KEYS

A C-key belongs to a master key system, but has a special code informing that it is a C-key. It also has a PKID but can not operate locks as a user key. There is always a master C-key with a special GR code. This is the first C-key.

For security reasons, C-keys are used for adding and deleting items in the A-list or the NA-list of a lock. In each lock, the identities of all C-keys that are allowed to make changes in the authorisation tables are recorded in the A-list. Thereby, it is possible to modify rights to different C-keys in different locks. However, C-keys do not contain any information on the user keys.

The Master C-key is used for changing the authorisations of C-keys. The Master C-key is recorded in all locks of a master key system. The Master C-key is also allowed to make changes of the user key authorisations.

The C-keys are also used to guarantee the security of data stored in the C-software. In combination with a

PIN code entered by a user, a C-key enables reading of encrypted data in the C-software.

If a C-key is lost, authorisations can be changed by means of the Master C-key. If the Master C-key is lost, the manufacturer delivers a new Master C-key. By means of this new Master C-key and the replace operation, the lost Master C-key can be replaced in all locks in the master key system and the C-software.

Use of C-keys

A C-key can be used in different ways for programming locks in a master key system. In the following, the different ways of programming locks will be described, partly with reference to figure 1.

Operations with C-Software

The C-Software of a lock system keeps track of the locks, keys, and their authorisations. If a modification is wanted, it is done in the C-Software of the customer computer 104 and is then downloaded to the C-key by means of the programming box 106 connected to the computer. The procedure at the lock is then as follows: The C-key is then inserted into a lock 20 where modifications are wanted during a specified time interval and the new information is transferred from the C-key to the lock 20.

Thus, when using the C-software, the information items regarding the updated user key authorisations are supplied from the C-software, stored in the C-key and supplied to the lock.

When an operation has been executed correctly for a specific lock, this is written to the C-key. It is then possible to update the status of the system in the C-Software database describing the system. In that way, the current status of the master keys system is always stored in the C-Software.

Operations with a programming device

If the C-Software is unavailable, it is possible to change the authorisation table of a lock by using a C-key and a programming device. This programming device can be the above-described box 106 operating disconnected from the computer 104. Alternatively, it is a dedicated portable box not shown in the figures and provided with a display and a keypad.

As an alternative, a low cost programming device can sometimes be used instead of the usual programming box. With this low cost alternative, only the delete, forbid and reauthorize operations are possible to perform.

To perform the add operation, an authorised C-key, a programming device and the key are needed. The key is needed because the SKID is needed in the A-list. The C-key can be either a separate key inserted into the box or integrated into the box. An add operation is then selected from a menu and this information is transferred to the lock.

It is also possible to perform other operations in a similar way, such as to authorise an entire group with such a solution by having one key of this group because all keys in a group have the same SKID.

To perform a delete operation, an authorised C-key and a programming device are needed. By means of the programming device, the PKIDs of keys in the A- and NA-lists are scrolled the key to be deleted selected. The key to be deleted is not required because it is possible to put the PKID of an authorised user key in the NA-list and to delete its PKID and SKID from the A-list, even without the user key present.

Thus, when using a programming device, the information items regarding the updated user key authorisations are supplied from the user key and directly to the lock.

<u>Operations without a programming device</u>

With just a C-key and a user key, it is possible change the authorisation of the user key in a lock. The C-key is first inserted into the lock for a specified time. The user key is then inserted into the lock. The C-key is then again inserted into the lock to confirm the update. Depending on the operation wanted, the C-key is inserted for different time intervals.

It is possible to delete all keys from the A-list. It is not possible to delete one single lost key from the A-list without deleting all keys in the list. However, it is possible to delete a key from the A-list if the key is present together with an authorised and programmed C-key.

The replace operation is possible to perform without a programming box. Thus, with a new key, a lost key can be replaced by means of the replace operation.

Like when using a programming device, the information items regarding the updated user key authorisations are supplied from the user key and directly to the lock.

Other operations possible with a C-key

It is possible to give a C-key some functions to execute when it is used with locks. It is possible to give a C-key the function of adding or deleting specific keys to the authorisation table. When issuing a number of new keys, it is thus possible for the manufacturer to supply a C-key with the new keys that functions to authorise all the new keys in some or all of the locks in a system. This would simplify the authorisation procedure significantly.

It should be noted that there are no links between the GR code of user keys and C-keys. However, it is possible to limit the use of C-keys to specific groups of a lock system.

D-Keys and M-Keys

D-keys (and M-keys) are used like C-keys. For certain operations, a D-key is required. As an example, at the distributor, when locks or keys are to be added to the system, D-software 204 authorised by D-key 202 is used together with downloading of necessary secret information from M-software 304The M-key is required when using the M-software.

The lock is then programmed at the customer either using the C-key 102 or by means of an adapter interconnecting the programming box 106 and the lock 20.

A preferred embodiment of a key and lock device has been described. It is realised that this can be varied within the scope as defined by the claims. Thus, although a cylinder lock device has been described, the invention is also applicable to other lock types as well, such as card locks.

Although an embodiment has been described, wherein both a public identification item and a secret identification item are stored in the A-list and the public identification item is stored in the NA-list, this could be varied. Thus, for example, it is entirely possible to store just public or just secret identification items in both lists or another combination thereof.

It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive.

THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

1. An electromechanical key and lock device, comprising:

- a key having a mechanical code and a key electronic circuitry comprising
  - a lock memory adapted for storing a public identification item of said key, and
  - a key contact; and
- a stand-alone lock having a lock electronic circuitry comprising
  - a lock memory,
  - a lock contact arranged to co-operate with said key contact, and
  - a blocking mechanism adapted to block operation of said lock unless an authorised key is inserted in the lock;

characterized in that

- said public identification item of said key comprises a group identification item identifying a group of keys having identical mechanical codes, and
- said lock memory is adapted for storing
  - a list of said public identification item and a secret identification item of authorised keys, and
  - a list of said public identification item of non-authorised keys,
- wherein a key is authorised if said public and secret identification items thereof are present in the list of authorised keys and said public identification item thereof is absent in the list of non-authorised keys.

2. The key and lock device according to claim 1, wherein said key and lock memories are arranged to store an electronic code field comprising said public identification item, said secret identification item and an encryption key.

3. The key and lock device according to claim 1 or 2, wherein said public identification item comprises a function identification item identifying one of the following functions: user key, customer authorisation key, distributor authorisation key, manufacturer authorisation key, and lock.

4. The key and lock device according to any of claims 1-3, wherein said public identification item comprises a device identification item identifying the different devices of a group and wherein the device identification item is unique in each group.

5. The key and lock device according to any of claims 1-4, wherein said secret identification item is identical for all devices within a group.

6. The key and lock device according to any of claims 1-5, wherein a public identification item stored in said list of authorised keys or said list of non-authorised keys comprising a device identification item of a specific value denotes an entire group.

7. The key and lock device according to any of claims 1-6, wherein secret identification items stored in said key memory can only be read by means of a special authorisation key.

8. The key and lock device according to any of claims 1-7, wherein a key is added to the number of authorised keys by adding its public and secret identification items to said list of authorised keys.

9. The key and lock device according to any of claims 1-8, wherein a key is deleted from the number of authorised keys by deleting its public and secret identification items from said list of authorised keys.

10. The key and lock device according to any of claims 1-9, wherein a key is deleted from the number of authorised keys by adding its public identification item to said list of non-authorised keys.

11. The key and lock device according to claim 10, wherein a key is added to the number of authorised keys by deleting its public identification item from said list of non-authorised keys.

12. The key and lock device according to any of claims 1-11, wherein a first key of the number of authorised keys is replaced by a second key by checking whether said first key is authorised, adding said public identification item thereof to said list of non-authorised keys and adding said public and secret identification items of said second key to said list of authorised keys.

13. The key and lock device according to any of claims 1-12, wherein a master authorisation key is recorded in said authorised list of all locks of a master key system.

14. A lock system, characterised by key and lock devices according to any of the preceding claims.

15. The lock system according to claim 14, comprising a customer database arranged to keep track of which keys are authorised in which locks in said lock system.

16. The lock system according to claim 14, comprising a distributor database including a key/lock register having an open part for display of open system information for design of changes and a secret part including authorisation codes and secret keywords used in the system.

17. The lock system according to claim 14, comprising at least one authorisation key used for programming the lock devices, said at least one authorisation key being authorised to update said information stored in said lock memory of lock devices.

18. A method of updating authorisation information of a lock device of a lock system according to any of claims 14-17, characterised by the step of updating said information in said lock memory of said lock device.

19. The method according to claim 18 when subordinated claim 15 or 16, comprising the following steps:

- transferring updating information from said customer or distributor database to an authorisation key; and
- transferring updating information from said authorisation key to said lock memory of a lock device.

20. The method according to claim 18, comprising the following steps:

- instructing an updating operation by inserting an authorisation key into said lock, and
- transferring updating information from a user key to said lock memory of said lock device.

21. The method according to any of claims 18-20, comprising the additional steps of

- verifying the updating operation by inserting said authorisation key into said lock, and

- transferring verification information from said authorisation key to said customer or distributor database.

22. An electromechanical key and lock device substantially as herein before described and with reference to the accompanying drawings.

23. A lock system substantially as herein before described and with reference to the accompanying drawings.

24. A method of updating authorisation information of a lock device of a lock system substantially as herein before described and with reference to the accompanying drawings.

Dated this thirtieth day of September 2004

Assa Abloy AB
Patent Attorneys for the Applicant:

F B RICE & CO

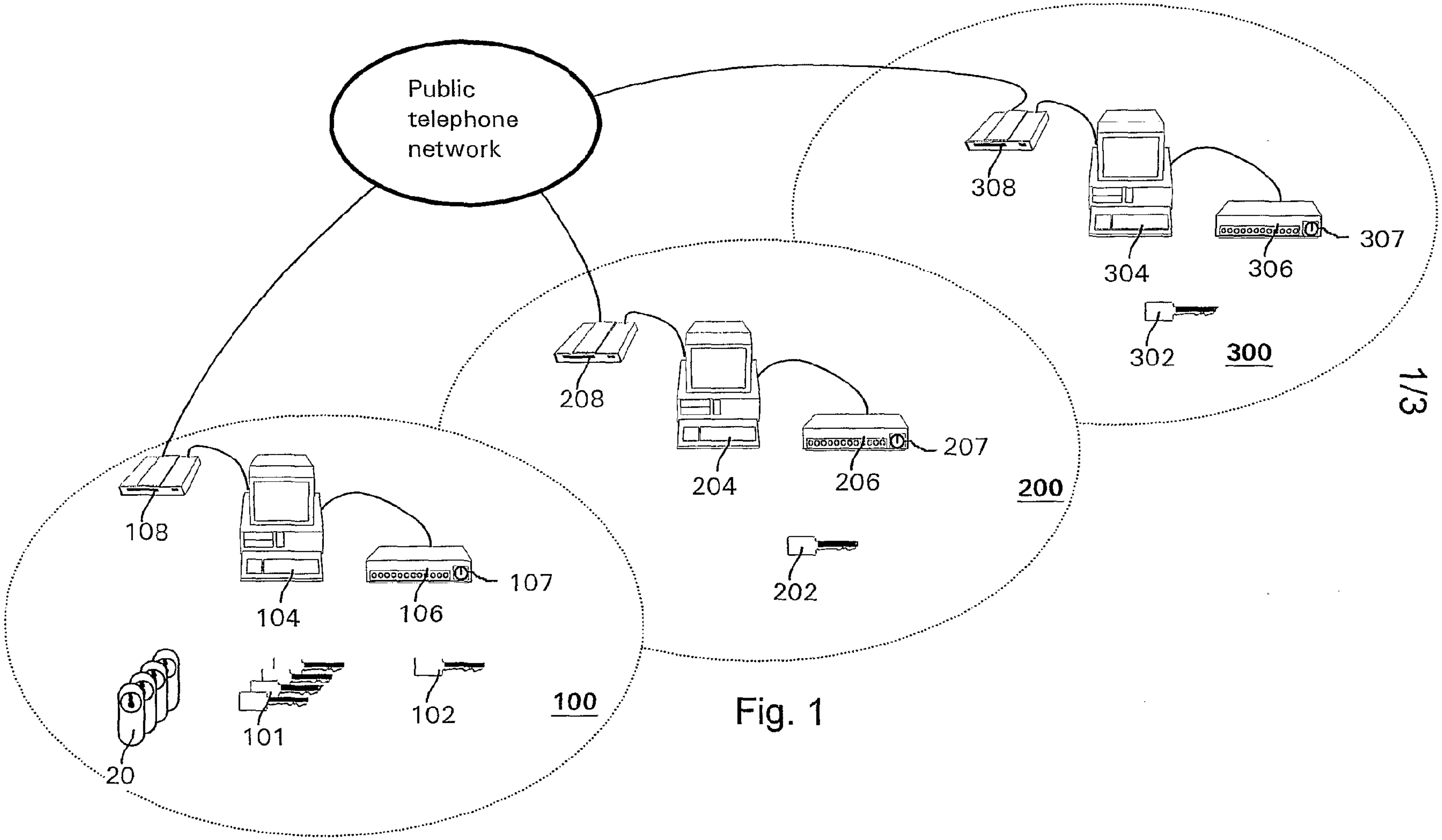

Public
telephone
network
308
304
306
307
302
300
208
204
206
207
200
202
108
104
106
107
100
20
101
102

Fig. 1

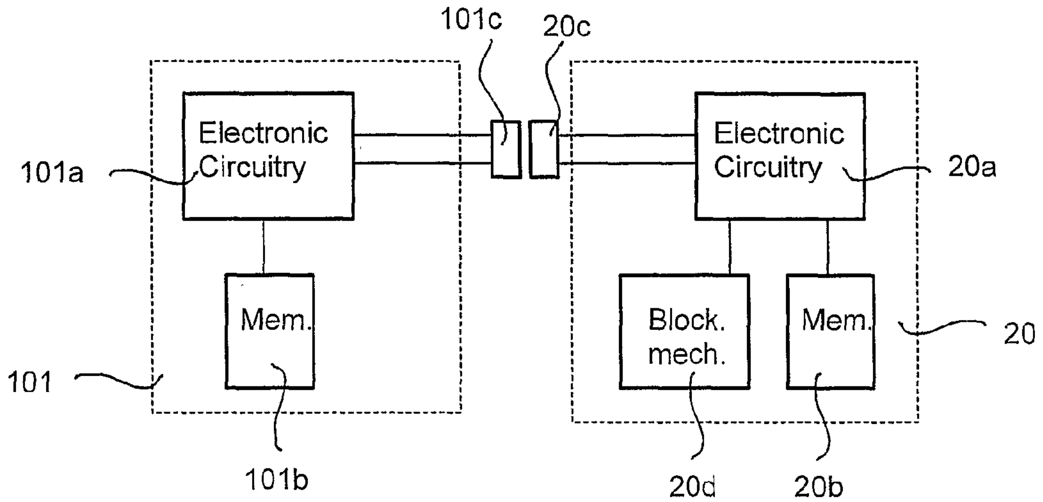

101c
20c
Electronic Circuitry
101a
Electronic Circuitry
20a
Mem.
Block. mech.
Mem.
20
101
101b
20d
20b

Fig. 2

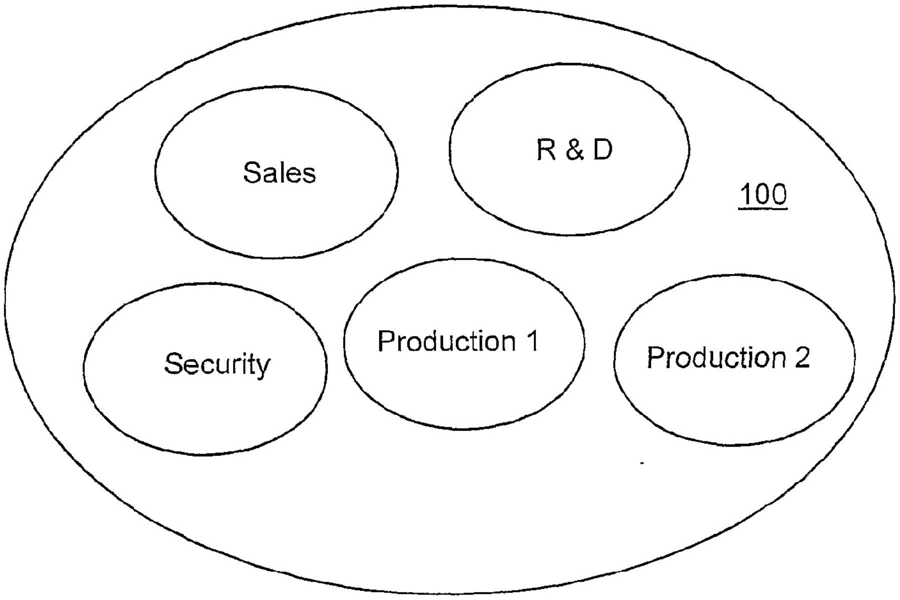

Sales
R & D
100
Security
Production 1
Production 2

Fig. 3

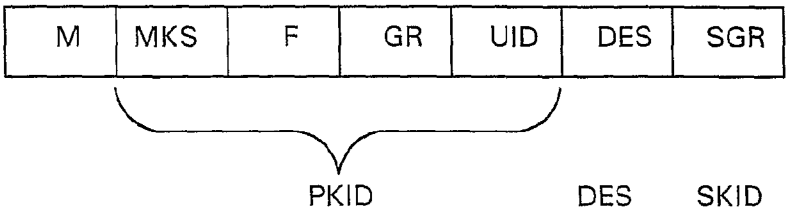


Fig. 4a

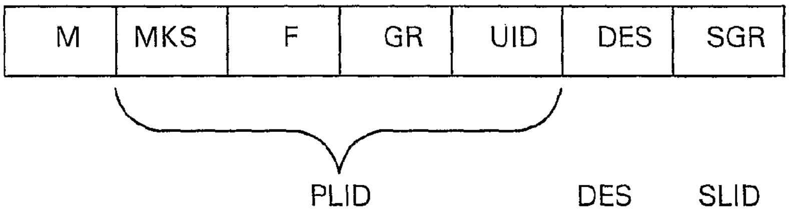


Fig. 4b

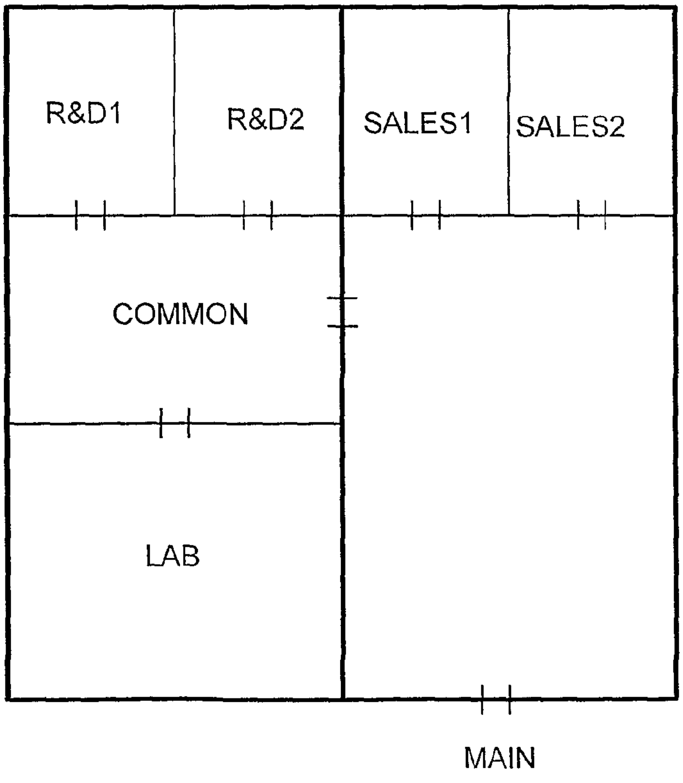


Fig. 5