Description

Background of the Invention

The present invention pertains to secure telecommunication systems and more particularly to an expandable hierarchical key management system which supports the delegation of authority for certification and authentication of users.

A typical key management system is shown in U.S. Pat. No. 4,578,531, issued March 25, 1986, to J. Everhart et al. This patent teaches a key distribution system connected to each of a plurality of secure terminals. When a secure data transmission is desired, each terminal must establish communication with the key distribution center. The key distribution center then establishes the terminal's credentials and performs the security analysis required.

The disadvantages of this system are that the key distribution center must be involved for each secure communication between any two terminals. The terminals exchange their security packets of information only through the key distribution center. Each terminal must send security information to the key distribution center for verification and receive subsequent information from the key distribution center. Such multiple communications are inefficient.

Further, the above-mentioned system provides no hierarchy of security. Since all critical keying data is contained at the center, if the key distribution center's security is compromised, each user's security is also compromised.

European Patent 0287720 (IBM) describes a method for simplifying key management and situations where you need crypto keying relationships are required and to end between pairs of parties and asymmetric encryption algorithm is to be used. It is useful in the cases where the parties come from disjoint subsets of the total population of parties. The method provides some of the characteristics of public key crypto system (PKS) utilizing the public identities of the parties as part of the key, but lacks the property of PKS which allows a party to independently generate a secret key which is known only to that party.

Accordingly, it is an object of the present invention to provide a hierarchical key distribution system which permits the establishing of security directly between terminal users.

Summary of the Invention

In accomplishing the object of the present, a novel hierarchical key distribution system is shown.

A hierarchical key management system certifies a plurality of users for secure communications via the public switched telephone network. The hierarchical key management system allocates users into defined user groups.

The hierarchical key management system includes groups of terminals. Each group of terminals corresponds to one of the groups of users. Each of the terminals permits secure communications by a number of users to other ones of the users through the public switched telephone network. Each of the users are previously certified by a common certifying authority. This certification comprises the generation of a set of asymmetric keys which are encrypted and modified to include the authorization predetermined time interval for which the certification is valid.

The hierarchical key management system includes a plurality of key certification authorities. The key certification authorities certify users of a user group for use of the terminals for secure communications with other users of said user group.

The hierarchical key management system also includes a key certification center. The key certification center is connected to each of the key certification authorities.

The key certification center grants certification authority to each of the key certification authorities and provides a means for authorizing secure communications between users of different user groups. As a result, the terminals are allowed to establish secure communications via the network, without connection to the common certifying authority.

Brief Description of the Drawings

Fig. 1 is a block diagram of a key distribution system embodying the principles of operation of the present invention.

FIG. 2 is a block diagram of a secure call setup between two secure wireline terminals served by the same key certification authority.

FIG. 3 is a block diagram of a secure call setup between two secure wireline terminals served by different

key certification authorities, but the same key certification center.

FIG. 4 is a block diagram of the key certification center and key certification authority.

Description of the Preferred Embodiment

Referring to FIG. 1, a key management system heirarchy is shown. Key certification center (KCC) is the central authority of this system. The KCC may comprise a dedicated special purpose computer system which includes a keyboard, display terminal, hard disk, backup tape streamer, printer and a network interface terminal (NIT). The NIT will be explained infra.

The KCC is connected to a number of key certification authorities (KCAs) Each KCA and the KCC includes a modem which provides for high-speed telephonic connection of the KCAs and KCC via the public switched telephone network. Other communication transmission media can also be employed. Three KCAs are shown in FIG. 1 local authority A, local authority B and local authority C. However, more than three KCAs may be connected to a KCC.

Each KCA also comprises a computer system including a keyboard, display terminal, hard disk, backup tape streamer, printer and network interface terminal. Each local authority or KCA is typically responsible for providing secure communications between up to 500 users, although a KCA may handle agreater number of users. For example, local authority A provides secure communications between the users of user group A. Each of the user groups A, B and C typically comprises up to 500 secure wireline terminals (SWTs). The SWTs are connected to the KCAs via modems which provide for high-speed telephonic connection of the SWTs of a group to their KCA. Other communication transmission media can be used. A user is an individual who is certified to use one or more of the SWTs within a user group.

Each SWT generates asymmetric keys for the secure exchange of traffic keys. The SWT employs a security activation device (SAD) for terminal access and user certification. The SAD is a physical key which is initially programmed by the KCA and subsequently reprogrammed by the SWT. The SAD is inserted into a receptacle of the SWT to enable secure communications and user authentication.

The SWT generates a unique asymmetric encrypt/decrypt key pair for each user. This asymmetric key pair is certified by the local authority (KCA). For large communications systems including more than one KCA, users from one user group may desire to call users in another user group. In this case, users who call inter group must be certified by KCA's which have been registered with a common KCC.

If a user's local authority (KCA) is temporarily out of service, the KCC can perform as a backup to any of the KCAs which are out of service. This is achieved by loading the backup tape of the KCA which is out of service into the KCC.

Initially a secure communications user is issued a seed SAD and corresponding password by his local authority (KCA). The seed SAD obtains its name from being a first or initial SAD from which other security information pertaining to an individual user is generated. The seed SAD contains data relating to the user's identification, and special codes necessary for certification.

A user may be certified by inserting his SAD into an SWT. Next, the user enters a password and when prompted places a call to the KCA which is his local authority. Using this SAD and password, a user may be certified on up to 8 SWTs. Further, up to 8 users may be certified on an individual SWT. The number of users per SWT and SWTs per user are typically set at eight, but flexability is provided for a greater number of users per SWT and SWTs per user.

Once a user has been certified on a particular SWT, he may make secure calls to other users within the same local authority or to other users which share a common KCC via an automated key generation and distribution process jointly performed by the two terminals. That is, a user in USER GROUP A may call another user in USER GROUP A or a user in USER GROUP A may call a user in USER GROUP B or USER GROUP C or vice versa. Once the SWT users are certified, the users may place a normal call through the public switched telephone network (PSTN) or other network. When it is determined that the call is to be a secure call, a secure push button is pressed on the SWT. The two SWTs in the particular call exchange certification data and generate and exchange traffic keys. Secure communications may now take place. As part of this synchronization and security process, authentication information such as the identity of the other party and security level of the connection is displayed on the SWT.

At the time of certification of a user, the KCA attaches an expiration code to the user's SAD or key which is being certified. Prior to the expiration of his SAD, the user will be notified to recertify his SAD. To recertify, the user will call his local KCA using his password and SAD. During the recertification, the terminal will generate a new asymmetric key pair encrypt/decrypt which will be certified by the KCA and a new expiration attached and stored in the user's SAD. If a user fails to recertify with the KCA prior to the expiration date, the SWT will automatically deny his access to the system.

Authority is delegated throughout this key management system. The KCC and the KCA do not contain the private key of each user or SWT. Therefore, if any one of the KCAs or the KCC is compromised, all users within the key management system are not compromised. However, the compromised KCC or KCA may give false certifications.

The delegation of authority is accomplished through a process in which the KCAs become registered with the KCC. This is accomplished by using a secure procedure over the PSTN. Once a KCA is registered with a KCC, the KCA may issue registration packets as part of its certification process of individual users. These registration packets allow users to communicate securely to users in different local authority groups (USER GROUP A, B or C).

A KCA will be required to execute a recertification process with the KCC at regular intervals to certify new asymmetric domain keys and to receive global unauthorized key information. The transactions that take place between the KCA and the KCC will be similar to the transactions between a SWT and a KCA for certification, except for message content.

The KCC maintains and distributes a global unauthorized key list (UKL). The distribution of the UKL is achieved through the system hierarchy. The KCAs receive the UKL from their respective SWT users. This data, a Lockout Packet, is then transmitted to the KCC to update the global UKL. The global UKL is then distributed through the KCAs to each SWT. Secure sessions with users on the UKL is automatically prevented by the SWT. If no KCC is present in the configuration, the UKL is stored within the KCA.

From the time a seed SAD is created by the KCA until it is zeroized (cleared or reset), lost or expires, the key management system monitors, modifies and accounts for the use of that SAD. Once users have been certified by a KCA, only terminal-to-terminal transmissions are necessary to establish a secure communication link between the two SWTs. These transmissions enable a secure channel to be established between the SWTs. When the user presses a secure push button of his SWT, a series of messages is exchanged between the SWTs. Some of this information exchanged indicates the channel characteristics of the SWT's modem.

Referring to FIG. 2, a secure call between SWT user 1A and SWT user 5A is shown. SWT users 1A and 5A are indicated as certified by the same authorizing authority, that is, KCA A as shown in FIG. 2. The description that follows assumes that SWT 1A and SWT 5A have previously certified their SAD (security activiation device) keys. This is indicated by the lines connecting SWTs 1A and 5A to KCA A and indicated by the CERTIFIED SAD key. At a prior time, both SWTs 1A and 5A have undergone this certification process.

SWTs 1A and 5A have previously established a connection through the telephone network. At this time, the user presses the secure push button on SWT 1A. This initiates an automatic message exchange via the PSTN that will result in a secure 2400 baud link being established between SWTs 1A and 5A. The 2400 baud link is given as an example. The data link which is established may be at any data rate practically achieved by the SWTs.

The following Table 1 lists abbreviations used for the various encrypt and decrypt vectors used hereinafter.

TABLE 1

Ex	-	USER'S ENCRYPT VECTOR
Dx	-	USER'S DECRYPT VECTOR
Exa	-	Key AUTHORITY'S ENCRYPT VECTOR
Dxa	-	Key AUTHORITY'S DECRYPT VECTOR
Eax	-	Key AUTHORITY'S CERTIFICATION ENCRYPT VECTOR
Dax	-	Key AUTHORITY'S CERTIFICATION DECRYPT VECTOR
Ec	-	Key CERTIFICATION ENCRYPT VECTOR
Dc	-	Key CERTIFICATION DECRYPT VECTOR
Exts	-	USER'S CERTIFICATION ENCRYPT VECTOR
Dxts	-	USER'S CERTIFICATION DECRYPT VECTOR

Each user has inserted his certified SAD key into the respective SWT. First, the two SWTs will exchange Access/Domain messages. These messages contain: an authority ID (the KCA identity), version number, an

expiration date for Dax, a center ID (KCC identity) version number, expiration date for Dc, terminal type and terminal serial number. Both SWTs will examine the message transmitted and will try to match common asymmetric domain keys, either Dax or Dc. A match will occur since both SADs have been certified by the KCA.

Next, each SWT sends the other an Authentication Packet message. The Authentication Packet message contains the following information: user's ID signature (IDS), user's ID, SAD serial number (SSN) access information, terminal serial number (TSN) and the user's certified asymmetric key Ext.

Each SWT will receive the other's Authentication Packet message and decrypt it using their common domain key Dax. As a result, each SWT will extract the other's asymmetric key Ext. The other user's ID is displayed on the SWT. The ID displayed also will indicate the lowest common classification that the two user's have. If critical mismatches are found in the access information, the call will be terminated.

Next, each SWT generates two duplicate copies of one Random Component (RC) that will be used in the keying of the Kg. One copy of the RC is loaded into the local transmit Kg. The other copy of the RC is encrypted using the other USERS Ext. Each SWT then transmits a Random Component message packet to the other USER which is encrypted with the other USER Ex. When each SWT receives the other's Random Component message packet, it will decrypt it using Dxt. The random component will be and used to key the receive Kg.

Lastly, a Crypto Sync (CS) message packet is generated by each SWT. SWTs 1A and 5A then exchange Crypto Sync message packets via the PSTN. Each SWT then processes the Crypto Sync message received from the other SWT. The Crypto Sync message is processed by the receive Kg to obtain crypto synchronization. When crypto synchronization is complete, each SWT notifies its user that a secure link has been established at the appropriate baud rate.

If the transmissions between the two SWTs occur at a 2400 baud rate, the security processing mentioned above will take approximately 10 seconds. Forward error correction is used for the data exchange to minimize the effects of impairments.

Turning to FIG. 3, a secure call from SWT user 1A to SWT user 7B will be explained. SWT user 1A has been certified by KCA A. SWT user 7B has been previously certified by KCA B. This is indicated by the dashed lines between SWT 1A and KCA A and between SWT 7B and KCA B, respectively. KCA A and KCA B have previously been certified by key certification center (KCC) X. As previously mentioned, SWT 1A and SWT 7B are interconnected in an unsecure fashion through the PSTN. The user of SWT 1A presses the secure push button and as a result, the Access/Domain message packets are transmitted between SWTs 1A and 7B. Since these Access/Domain messages contain the KCC ID and version, the Access/Domain message packets will match. Secure calls between SWTs in different KCCs are not permitted under this system.

Since the match was detected on the identity of the KCC and not the KCA, the next message transmission between the SWTs will be different than that mentioned above for a common KCA. The next message packet transmitted between the SWTs in this case is called a Registration Packet. The Registration Packet contains the following information: the authorizing KCA's asymmetric domain key (Dax), the KCA's ID and access information pertinent to each KCA. The entire Registration Packet is encrypted using the KCC's domain key Ec. Each SWT will receive the other's Registration Packet and decrypt it using the common domain key Dc. As a result, each SWT will extract the other's asymmetric domain key, Dax. When each SWT determines that the other's KCC identity and version correctly match, the security processing will occur as mentioned above. If the KCC's ID and version do not match, the secure call will be terminated.

After the Registration Packet message has been properly decrypted, authentication message packets will be exchanged between SWTs 1A and 7B. The processing for the Authentication Packet message occurs as described above for the case of the common KCA. Next, the Random Component message packets are exchanged between SWTs 1A and 7B. Again, the processing is as explained above for the common KCA. Lastly, Crypto Sync message packets are exchanged between SWTs 1A and 7B and processed as mentioned above.

For the case of a secure call between SWTs in different KCA domains, but in a common KCC domain, and assuming a transmission rate of 2400 baud, the time required to set up a secure call between the two SWTs will be approximately 15 seconds.

As shown in FIG. 1, when a KCA is out of service, the KCC under which that KCA is certified may act as a backup KCA. USER GROUP BACKUP may be provided to any user group such as USER GROUP A, B or C. To accomplish this, the backup tape of the KCA which is out of service is loaded into the KCC. For certification of users in this configuration, the KCC acts as a KCA.

The initial certification of a KCA occurs in a similar fashion to that of the initial certification by a KCA of a SAD on an SWT. For the initial certification of a KCA, a secure link is established using a password and a seed SAD for that particular KCA. For example, KCA A or local authority A establishes a secure link to the central authority KCC. When the secure link is established, the KCA sends a certification information packet. This packet contains the authority's identification signature (IDS) terminal serial number (TSN), Exa, Dax and a SAD serial number (SSN).

The KCC responds to the KCA with a Registration Packet which certifies the KCA to act for the KCC in certifying users. In addition, the KCC sends to the KCA a Lockout Packet, which is the unauthorized key list and the global decryption key Dc. The Registration Packet contains newly generated asymmetric domain keys which are encrypted with the KCC's Ec. The Registration Packet also contains the KCA's identification, and access/clearance information.

When the authorization period for a particular KCA's asymmetric domain keys expires, the KCA will recertify new keys with the KCC. The recertification process is essentially the same as the initial certification process except that the global asymmetric domain key Dc is not sent by the KCC, if the certification period previously set has not yet expired.

After the certification of the user by the KCA, the particular SWT on which that user is certified generates a SAD cover component, which is randomly generated, and stores the access domain message encoded or covered by the SAD cover component in non-volatile memory of the SWT. Next, the SWT stores the authentication packet, the Registration packet the TSN (terminal serial number) and the cover component on the SAD. The SWT also stores the unauthorized key list (UKL), and the decrypt vectors Dc and Dxt covered with the same SAD cover component. With each use, the SAD cover component is updated.

Referring to FIG. 4, a block diagram of a KCC or KCA is shown. Each KCA and the KCC may comprise a computer controlled system. The computer control system includes a CPU, hard disk, backup tape unit, printer, keyboard, display, and network interface terminal (NIT). The NIT is a secure wireline terminal specially adapted to interface to a KCC or a KCA. The NIT includes a modem which is connected to any user's modem, in the case of a KCA, or is connected to a KCA, in case of a KCC. Each modem connection is accomplished via the public switched telephone network.

The control console shown in FIG. 4 includes the display, the keyboard, the CPU, the hard disk, and the backup tape unit. The CPU is connected to the disk, to to the backup tape unit, to the display and to the keyboard. In addition, the printer is connected to the CPU.

Lastly, the NIT is connected to the CPU. The NIT provides for high-speed data transfer between users and a KCA or between a KCA and a KCC. The NIT also provides for high-speed communications directly between users and a KCC which is acting as a KCA in the backup mode.

Each NIT and SWT includes a modem. These modems are capable of sending data at high speeds, such as 2400 to 9600 baud, although not limited to these speeds.

The keyboard provides for data input to the CPU. The display provides for visual output from the CPU. The printer provides for hard copy visual display of CPU output. The disk provides for storing all the operating software and data base concerning the SWTs and in the case of a KCC, it stores information pertinent to the KCAs. The backup tape unit provides for loading KCA information into a KCC which is out of service so that the KCC may provide the functions of the KCA. In addition, the backup tape unit may provide for reloading the system in case of a KCA or KCC being out of service.

Claims

1. A hierarchical key management system for enabling ones of a plurality of users to establish secure communications via a switching network (PSTN), said hierarchical key management system comprising:

   predefined user groups (A,B,C) of said users;

   characterized in that:

   each of said users being previously certified by a common authority, said certification comprising the generation of a set of asymmetric keys which are encrypted and modified to include the authorization predetermined time interval for which said certification is valid;

   terminal means (1-500) connected to said switching network (PSTN), said terminal means for establishing secure communications through said switching network;

   groups of terminal means (A,B,C), each group corresponding to said group of users, a first terminal means establishing communications with a second terminal means via said switching network; and

   said first (1) and second (2) terminal means directly establishing secure communications via said switching network, without connection to said common authority.

2. A hierarchical key management system as claimed in claim 1, said common authority including:

   a plurality of key certification authority means (A,B,C) for certifying said users of a user group (A,B,C), each of said key certification authority means (A,B,C) corresponding to a user group and to a terminal means group (A,B,C), each key certification authority means certifying its corresponding users for use of said terminal means for direct secure communications with other users of said user group, each

* C L M S *

The KCC responds to the KCA with a Registration Packet which certifies the KCA to act for the KCC in certifying users. In addition, the KCC sends to the KCA a Lockout Packet, which is the unauthorized key list and the global decryption key Dc. The Registration Packet contains newly generated asymmetric domain keys which are encrypted with the KCC's Ec. The Registration Packet also contains the KCA's identification, and access/clearance information.

When the authorization period for a particular KCA's asymmetric domain keys expires, the KCA will re-certify new keys with the KCC. The recertification process is essentially the same as the initial certification process except that the global asymmetric domain key Dc is not sent by the KCC, if the certification period previously set has not yet expired.

After the certification of the user by the KCA, the particular SWT on which that user is certified generates a SAD cover component, which is randomly generated, and stores the access domain message encoded or covered by the SAD cover component in non-volatile memory of the SWT. Next, the SWT stores the authentication packet, the Registration packet the TSN (terminal serial number) and the cover component on the SAD. The SWT also stores the unauthorized key list (UKL), and the decrypt vectors Dc and Dxt covered with the same SAD cover component. With each use, the SAD cover component is updated.

Referring to FIG. 4, a block diagram of a KCC or KCA is shown. Each KCA and the KCC may comprise a computer controlled system. The computer control system includes a CPU, hard disk, backup tape unit, printer, keyboard, display, and network interface terminal (NIT). The NIT is a secure wireline terminal specially adapted to interface to a KCC or a KCA. The NIT includes a modem which is connected to any user's modem, in the case of a KCA, or is connected to a KCA, in case of a KCC. Each modem connection is accomplished via the public switched telephone network.

The control console shown in FIG. 4 includes the display, the keyboard, the CPU, the hard disk, and the backup tape unit. The CPU is connected to the disk, to to the backup tape unit, to the display and to the keyboard. In addition, the printer is connected to the CPU.

Lastly, the NIT is connected to the CPU. The NIT provides for high-speed data transfer between users and a KCA or between a KCA and a KCC. The NIT also provides for high-speed communications directly between users and a KCC which is acting as a KCA in the backup mode.

Each NIT and SWT includes a modem. These modems are capable of sending data at high speeds, such as 2400 to 9600 baud, although not limited to these speeds.

The keyboard provides for data input to the CPU. The display provides for visual output from the CPU. The printer provides for hard copy visual display of CPU output. The disk provides for storing all the operating software and data base concerning the SWTs and in the case of a KCC, it stores information pertinent to the KCAs. The backup tape unit provides for loading KCA information into a KCC which is out of service so that the KCC may provide the functions of the KCA. In addition, the backup tape unit may provide for reloading the system in case of a KCA or KCC being out of service.

Claims

1. A hierarchical key management system for enabling ones of a plurality of users to establish secure communications via a switching network (PSTN), said hierarchical key management system comprising:

predefined user groups (A,B,C) of said users;

characterized in that:

each of said users being previously certified by a common authority, said certification comprising the generation of a set of asymmetric keys which are encrypted and modified to include the authorization predetermined time interval for which said certification is valid;

terminal means (1-500) connected to said switching network (PSTN), said terminal means for establishing secure communications through said switching network;

groups of terminal means (A,B,C), each group corresponding to said group of users, a first terminal means establishing communications with a second terminal means via said switching network; and

said first (1) and second (2) terminal means directly establishing secure communications via said switching network, without connection to said common authority.

2. A hierarchical key management system as claimed in claim 1, said common authority including:

a plurality of key certification authority means (A,B,C) for certifying said users of a user group (A,B,C), each of said key certification authority means (A,B,C) corresponding to a user group and to a terminal means group (A,B,C), each key certification authority means certifying its corresponding users for use of said terminal means for direct secure communications with other users of said user group, each

of said plurality of key certification authority means being connected to said terminal means of said corresponding group; and

key certification center means (KCC) connected to each of said plurality of key certification authority means, said certification center means (KCC) for granting certification authority to each of said key certification authority means for authorizing direct secure communications between terminal means of different groups (A,B,C).

3. A hierarchical key management system as claimed in claim 2, wherein there is further included security activation device means (SAD) corresponding to an individual user and being connectable to said terminal means, said security activation device means operating to store authentication, encryption and decryption information for transmission to said terminal means.

4. A hierarchical key management system as claimed in claim 3, said security activation device means (SA) further connected to said terminal means (1-500) to enable said terminal means to program said security activation device means with certification information.

5. A hierarchical key management system as claimed in claim 4, said security activation device means (SAD) being further connected to said terminal means to permit said terminal means (1-500) to repetitively reprogram said security activation device means with regenerated communication information.

6. A hierarchical key management system as claimed in claim 2, wherein said users (1-500) of a user group (A,B,C) are directly connected to said key certification center means (KCC) for the condition of the user group's key certification authority means being out of service.

7. A method for secure communications via a telephone network between at least two terminals (1-2) of a plurality of terminals, [previous certification from a common authority (KCA, KCC)] prior to communication with one another having certification, said certification comprising [said method compromising] the steps of:

characterized in that:

generating a set of asymmetric domain keys which are encrypted and modified to include the authorization predetermined time interval for which said certification is valid from a common authority;

completing a connection via the telephone network for the transmission of information between said two terminals (1-2);

exchanging encrypt key between said two terminals (1-2), under an encrypt key of said common authority (KCA,KCC);

determining a transmit and key pair for each terminal, to allow secure communications between said two connected terminals (1-2); and

saving a second modified encrypt/decrypt key pair, specific to each terminal, for subsequent secure communications.

8. A method for secure communications as claimed in claim 7, wherein there is further included the step of inserting a security activation device (SAD) into said terminals for insuring that each user (1-500) of the corresponding terminal (1-500) is certified for secure communications.

9. A method for secure communications as claimed in claim 8, wherein there is further included the step of verifying information contained on said security activation device (SAD) by said terminal to insure that said user is presently certified.

10. A method for secure communication as claimed in claim 7, wherein there is further included the step of establishing without subsequent connection to said common authority a session key directly between said two terminals.

Patentansprüche

1. Ein hierarchisches Schlüsselverteilungssystem, um irgendwelchen einer Mehrzahl von Benutzern zu ermöglichen, sichere Verbindungen über ein Wählnetzwerk (PSTN) herzustellen, wobei das genannte hierarchische Schlüsselverteilungssystem umfaßt:
vordefinierte Benutzergruppen (A, B, C) der genannten Benutzer;

dadurch gekennzeichnet, daß jeder der genannten Benutzer vorhergehend von einer gemeinsamen Autorität bestätigt worden ist, die genannte Bestätigung das Erzeugen eines Satzes von asymmetrischen Schlüsseln umfaßt, die chiffriert und modifiziert sind, um das vorbestimmte Bestätigungszeitintervall einzuschließen, währenddessen die genannte Bestätigung gültig ist;
Anschlußeinrichtungen (1-500), die mit dem genannten Wählnetz (PSTN) verbunden sind, wobei die genannten Anschlußeinrichtung zum Herstellen von sicheren Verbindungen durch das genannte Wählnetz hindurch sind;
Gruppen von Anschlußeinrichtungen (A, B, C), wobei jede Gruppe einer der genannten Benutzergruppen entspricht, wobei eine erste Anschlußeinrichtung Verbindungen mit einer zweiten Anschlußeinrichtung über das genannte Wählnetz herstellt; und
die genannte erste (1) und zweite (2) Anschlußeinrichtung unmittelbar sichere Verbindungen über das genannte Wählnetz ohne Verbindung mit der genannten gemeinsamen Autorität herstellen.

2. Ein hierarchisches Schlüsselverteilungssystem, wie in Anspruch 1 beansprucht, wobei die gemeinsame Autorität enthält:
eine Mehrzahl von Schlüsselbestätigungsautoritätseinrichtungen (A, B, C) zum Bestätigen der genannten Benutzer einer Benutzergruppe (A, B, C), wobei jede der genannten Schlüsselbestätigungsautoritätseinrichtungen (A, B, C) einer Benutzergruppe und einer Anschlußeinrichtungsgruppe (A, B, C) entspricht, jede Schlüsselbestätigungsautoritätseinrichtung ihre entsprechenden Benutzer zur Benutzung der genannten Anschlußeinrichtung für direkte, sichere Verbindungen mit anderen Benutzern der genannten Benutzergruppe bestätigt, jede der genannten Mehrzahl von Schlüsselbestätigungsautoritätseinrichtungen mit der genannten Anschlußeinrichtung der genannten entsprechenden Gruppe verbunden ist; und
eine Schlüsselbestätigungszentraleinrichtung (KCC), die mit jeder der genannten Mehrzahl von Schlüsselbestätigungsautoritätseinrichtungen verbunden ist, wobei die genannte Bestätigungszentraleinrichtung (KCC) zum Verleien einer Bestätigungsautorität an jede der genannten Schlüsselbestätigungsautoritätseinrichtungen zum Bevollmächtigen direkter, sicherer Verbindungen zwischen Anschlußeinrichtungen unterschiedlicher Gruppen (A, B, C) ist.

3. Ein hierarchisches Schlüsselverteilungssystem, wie in Anspruch 2 beansprucht, in der ferner ein Sicherheitsbetätigungseinrichtungsmittel (SAD) enthalten ist, das einem einzelnen Benutzer entspricht und mit der genannten Anschlußeinrichtung verbindbar ist, wobei das genannte Sicherheitsbetätigungseinrichtungsmittel arbeitet, Autentizitäts-, Chiffrier- und Dechiffrier-Informationen zur Übertragung zu der genannten Anschlußeinrichtung speichert.

4. Ein hierarchisches Schlüsselverteilungssystem, wie in Anspruch 3 beansprucht, wobei das genannte Sicherheitsbetätigungseinrichtungsmittel (SAD) ferner mit der genannten Anschlußeinrichtung (1-500) verbunden ist, um die genannte Anschlußeinrichtung zu befähigen, das genannte Sicherheitsbetätigungseinrichtungsmittel mit der Bestätigungsinformation zu programmieren.

5. Ein hierarchisches Schlüsselverteilungssystem, wie in Anspruch 4 beansprucht, wobei das genannte Sicherheitsbetätigungseinrichtungsmittel (SAD) ferner mit der genannten Anschlußeinrichtung verbunden ist, um der genannten Anschlußeinrichtung (1-500) zu erlauben, wiederholt das genannte Sicherheitsbetätigungseinrichtungsmittel mit erneut erzeugter Verbindungsinformation erneut zu programmieren.

6. Ein hierarchisches Schlüsselverteilungssystem, wie in Anspruch 2 beansprucht, in dem die genannten Benutzer (1-500) einer Benutzergruppe (A, B, C) direkt mit der genannten Schlüsselbestätigungszentraleinrichtung (KCC) unter der Bedingung verbunden sind, daß die Schlüsselbestätigungsautoritätseinrichtung für die Benutzergruppe außer Betrieb ist.

7. Ein Verfahren für sichere Übertragungen über ein Telefonnetz zwischen wenigstens zwei Endstationen (1-2) einer Mehrzahl von Endstationen, [vorausgehende Bestätigung von einer gemeinsamen Autorität (KCA, KCC)] die vor der Verbindung miteinander, eine Bestätigung haben, wobei die genannte Bestätigung umfaßt [das genannte Verfahren umfassend] die Schritte:
gekennzeichnet durch
Erzeugen eines Satzes von asymmetrischen Bereichsschlüsseln, die chiffriert und abgeändert sind, um das vorbestimmte Zeitintervall der Autorisierung einzuschließen, für das die genannte Bestätigung von einer gemeinsamen Autorität gültig ist;
Vervollständigen einer Verbindung über das Telefonnetz zur Übertragung von Informationen zwischen den genannten zwei Endstationen (1-2);

* C L M S *

Austauschen eines Chiffrierschlüssel zwischen den genannten zwei Endstationen (1-2) unter einem Chiffrierschlüssel der genannten gemeinsamen Autorität (KCA, KCC);
Bestimmen eines Übertragungs- und Schlüsselpaares für jede Endstation, um sichere Verbindungen zwischen den genannten zwei verbundenen Endstationen (1-2) zu ermöglichen; und
Aufheben eines zweiten, abgeänderten Chiffrier/Dechiffrier-Schlüsselpaares, das für jede Endstation spezifisch ist, für nachfolgende, sichere Verbindungen.

8. Ein Verfahren für sichere Verbindungen, wie in Anspruch 7 beansprucht, in dem ferner der Schritt des Einführens einer Sicherheitsbetätigungseinrichtung (SAD) in die genannten Endstationen eingeschlossen ist, um sicherzustellen, daß jeder Benutzer (1-500) der entsprechenden Endstation (1-500) zu sicheren Verbindungen bestätigen wird.

9. Ein Verfahren für sichere Verbindungen, wie in Anspruch 8 beansprucht, in dem ferner der Schritt zum Verifizieren von Informationen, die in der genannten Sicherheitsbetätigungseinrichtung (SAD) enthalten sind, durch die genannte Endstation eingeschlossen ist, um sicherzustellen, daß der genannte Benutzer gegenwärtig bestätigt ist.

10. Ein Verfahren zur sicheren Verbindung, wie in Anspruch 7 beansprucht, in dem ferner der Schritt enthalten ist, ohne nachfolgende Verbindung mit der genannten gemeinsamen Autorität einen Arbeitssitzungsschlüssel direkt zwischen den genannten zwei Endstationen herzustellen.

Revendications

1. Système hiérarchique de gestion par clés permettant à un parmi une pluralité d'utilisateurs d'établir des communications protégées via un réseau commuté (PSTN), ledit système hiérarchique de gestion par clés comprenant des groupes prédéfinis d'utilisateurs (A, B, C) desdits utilisateurs, système caractérisé en ce que :
   - chacun desdits utilisateurs est précédemment certifié par un organisme officiel commun, ladite certification comprenant la génération d'un ensemble de clés asymétriques qui sont codées et modifiées pour comprendre l'intervalle de temps prédéterminé d'autorisation pour lequel ladite certification est valide;
   - des moyens de terminal (1 à 500) raccordés audit réseau commuté (PSTN), lesdits moyens de terminal établissant des communications protégées via ledit réseau commuté;
   - des groupes de moyens de terminal (A, B, C), chaque groupe correspondant audit groupe d'utilisateurs, un premier moyen de terminal établissant des communications avec un second moyen de terminal via ledit réseau commuté; et
   - ledit premier (1) et ledit second (2) moyens de terminal établissent directement des communications protégées via ledit réseau commuté sans connexion audit organisme officiel commun.

2. Système hiérarchique de gestion par clés selon la revendication 1, dans lequel ledit organisme officiel commun comprend :
   - une pluralité de moyens d'organisme officiel de certification de clés (A, B, C) pour certifier lesdits utilisateurs d'un groupe d'utilisateurs (A, B, C), chacun desdits moyens d'organisme officiel de certification de clés (A, B, C) correspondant à un groupe d'utilisateurs et à un groupe de moyens de terminal (A, B, C), chaque moyen d'organisme officiel de certification de clé certifiant ses utilisateurs correspondant pour l'utilisation desdits moyens de terminal pour des communications protégées directes avec les autres utilisateurs dudit groupe d'utilisateurs, chacun de ladite pluralité de moyens d'organisme officiel de certification de clé étant raccordé audit moyen de terminal dudit groupe correspondant; et
   - un moyen central de certification de clé (KCC) raccordé à chacun de ladite pluralité de moyens d'organisme officiel de certification de clé, ledit moyen central de certification (KCC) accordant l'organisme officiel de certification à chacun desdits moyens d'organisme officiel de certification de clé pour autoriser des communications protégées directes entre les moyens de terminal de différents groupes (A, B, C).

3. Système hiérarchique de gestion par clés selon la revendication 2, comprenant de plus un moyen de dispositif d'activation de sécurité (SAD) correspondant à un utilisateur individuel et pouvant être connecté

* C L M S *

auxdits moyens de terminal, ledit moyen de dispositif d'activation de sécurité servant à stocker une information d'identification, de codage et de décodage pour une transmission auxdits moyens de terminal.

4. Système hiérarchique de gestion par clés selon la revendication 3, ledit moyen de dispositif d'activation de sécurité (SAD) étant raccordé, de plus, auxdits moyens de terminal (1 à 500) pour permettre auxdits moyens de terminal de programmer ledit moyen de dispositif d'activation de sécurité par l'information de certification.

5. Système hiérarchique de gestion par clés selon la revendication 4, ledit moyen de dispositif d'activation de sécurité (SAD) étant raccordé, de plus, auxdits moyens de terminal pour permettre auxdits moyens de terminal (1 à 500) de reprogrammer, de façon répétitive, ledit moyen de dispositif d'activation de sécurité à l'aide de l'information de communication régénérée.

6. Système hiérarchique de gestion par clés selon la revendication 2, dans lequel lesdits utilisateurs (1 à 500) d'un groupe d'utilisateurs (A, B, C) sont directement connectés audit moyen central de certification de clé (KCC) dans le cas où le moyen d'organisme officiel de certification de clé du groupe d'utilisateurs est hors service.

7. Procédé pour des communications protégées via un réseau téléphonique entre au moins deux terminaux (1-2) d'une pluralité de terminaux (certification précédente d'un organisme officiel commun (KCA, KCC)) avant une communication l'un avec l'autre possédant une certification, ladite certification comprenant (ledit procédé comprenant) les étapes caractérisantes suivantes :
   - la génération d'un ensemble de clés de domaine asymétrique qui sont codées et modifiées pour inclure l'intervalle de temps prédéterminé d'autorisation pour lequel ladite certification est valide à partir d'un organisme officiel commun;
   - l'achèvement d'une connexion via le réseau téléphonique pour la transmission de l'information entre lesdits deux terminaux (1-2);
   - l'échange d'une clé codée entre lesdits deux terminaux (1-2) sous une clé codée dudit organisme officiel commun (KCA, KCC);
   - la détermination d'une transmission et d'une paire de clés pour chaque terminal permettant des communications protégées entre lesdits deux terminaux connectés (1-2); et
   - la sauvegarde d'une seconde paire de clés modifiées de codage/décodage, spécifique à chaque terminal, pour des communications protégées suivantes.

8. Procédé pour des communications protégées selon la revendication 7, comprenant, de plus, une étape d'insertion d'un dispositif d'activation de sécurité (SAD) dans lesdits terminaux pour s'assurer que chaque utilisateur (1 à 500) du terminal correspondant (1 à 500) est certifié pour des communications protégées.

9. Procédé pour des communications protégées selon la revendication 8, comprenant, de plus, une étape de vérification de l'information contenue dans ledit dispositif d'activation de sécurité (SAD) par ledit terminal pour s'assurer que ledit utilisateur est présentement certifié.

10. Procédé pour des communications protégées selon la revendication 7, comprenant, de plus, une étape d'établissement direct d'une clé de cession entre lesdits deux terminaux sans connexion suivante audit organisme officiel commun.