

one of said pre-encrypted messages and including a first equipment ID in an encrypted form and one of said Sequence numbers in an encrypted form, said identifying block including a second equipment ID in a non-encrypted form;

- (b) decrypting at a communication service provider, said encrypted block by a first processor to obtain said first equipment ID and said sequence number;
- (c) evaluating by said first processor, said first and second equipment IDs to detect correspondence therebetween;
- (d) evaluating by said first processor, said sequence number with a previously used sequence number to detect a correspondence therebetween; and
- (e) denying access to said communication service when said step (c) fails to detect said correspondence or said step (d) detects said correspondence.

10. A method as claimed in claim 9 wherein:

said encrypted block additionally includes an error detection code;

said step (b) additionally obtains said error detection code;

said steps (c) and (d) additionally evaluate said error detection code to determine when an error is indicated; and

said step (e) denies access to said communication service when said step (c) or said step (d) determines that said error is indicated.

11. A method as claimed in claim 9 wherein:

said encrypted block additionally includes first user identification data (ID);

said step (b) additionally obtains said first user ID;

said method additionally comprises the step of maintaining a list of second user IDs;

said step (c) additionally evaluates said first user ID and said list of second user IDs to determine whether said first user ID is included in said list of second user IDs; and

said step (d) additionally determines whether to grant access to said communication service in response to said evaluation of said list of second user IDs with respect to said first user ID.

12. A method as claimed in claim 11 wherein said list of second user IDs serves as an unauthorized user list, and said step (d) denies access to said communication service when said first user ID is included in said list of second user IDs.

13. A method as claimed in claim 9 wherein:

said first equipment ID is encrypted using a secret key;

said method additionally comprises step of receiving a public key from a remote location, said public key complementing said secret key; and

said step (b) utilizes said public key in decrypting said encrypted block by said first processor.

14. A method as claimed in claim 13 wherein:

said communication service is a communication service provided through a network having a plurality of central switching offices in data communication with one another, each of said central switching offices in communication with its own plurality of base stations; and

said method additionally comprises steps of: providing an authentication center in data communication with said

central switching offices and said base stations, generating said complementing secret and public keys at said authentication center,

forming said encryption block at said authentication center, and

sending said public key from said authentication center to at least one of said central switching offices and said base stations.

15. A method as claimed in claim 9 wherein said log-on message additionally includes expiration date data, and said method additionally comprises steps of: saving first and second decryption keys in a memory contained in said authentication station; and selecting, in response to said expiration date data, one of said first and second decryption keys for use in said step (b).

16. A method as claimed in claim 9 wherein:

said communication service is provided through a network having a plurality of central switching offices, each of said central switching offices in communication with its own plurality of base stations; and

said steps (b), (c), (d) and (e) are performed at said base stations of said network.

17. A method as claimed in claim 9 wherein:

said communication service is provided through a network having a plurality of central switching offices, each of said central switching offices in communication with its own plurality of base stations; and

said steps (b), (c), (d) and (e) are performed at said central switching offices.

18. A system for providing communication services only to authenticated user terminals for use by users through a communication network having a plurality of nodes, said communication services being provided through said user terminals having pre-encrypted messages stored therein, said pre-encrypted messages including sequence numbers and equipment identification data (ID) associated with said user terminals, said system comprising:

one or more authentication modules, each authentication module for combining with a corresponding one of said user terminals; and

means, responsive to said equipment IDs, for producing said authentication modules, each of said authentication modules for storing an encrypted block of data therein, said encrypted block of data including said equipment ID in an encrypted form and a series of said sequence numbers in an encrypted form, said sequence numbers comprising a list of numbers in a particular order.

19. A system as claimed in claim 18 wherein said producing means is in data communication with said communication network, said producing means for generating complementary encryption and decryption keys, said encryption keys being used in forming said encrypted blocks and said decryption keys being transmitted to said network.

20. A system as claimed in claim 19, at least some of said network nodes for:

receiving said decryption keys and receiving log-on messages, wherein each message includes one of said authentication module encrypted blocks and one of said user terminal equipment IDs;

decrypting said encrypted blocks using said decryption keys;

evaluating whether said equipment IDs from said encrypted blocks corresponds to said equipment IDs from said user terminals;