

in memory that are executable by the processor to present a token set to the user, wherein the token set comprises at least two tokens, and wherein each token in the token set comprises at least two symbols that belong to the set of symbols, require the user to select a token from the token set for each pin position in the predetermined passcode, and authenticate the user based on the tokens that the user selected.

[22a] In accordance with an embodiment of the disclosure, the user is authenticated if: the number of tokens selected by the user is equal to the number of symbols in the passcode, at least one of the tokens selected contains a respective one of the passcode symbols, and the pin position of each of the selected tokens that contains a respective one of the passcode symbols corresponds to the pin position of its respective passcode symbol in the passcode.

[23] Additional advantages, objects, and features of the invention will be set forth in part in the description which follows and in part will become apparent to those having ordinary skill in the art upon examination of the following or may be learned from practice of the invention. The objects and advantages of the invention may be realized and attained as particularly pointed out in the appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

[24] The invention will be described in detail with reference to the following drawings in which like reference numerals refer to like elements wherein:

[25] Figure 1A is a block diagram illustrating an exemplary interception-proof authentication/ encryption system that can be incorporated into a device or a server that is accessed by a client system, in accordance with one embodiment of the present invention;

[26] Figure 1B is a block diagram illustrating the interception-proof authentication/encryption system incorporated into a device, in accordance with one embodiment of the present invention;

WHAT IS CLAIMED IS:

1. A method of allowing a user access to electronically stored information ("authenticating") using a predetermined electronically stored passcode ("passcode") that comprises a predetermined number of symbols ("passcode symbols") selected from a set of symbols, wherein each of the passcode symbols is characterized by a predetermined pin position, comprising:

presenting a token set to the user via a user interface of an electronic device, wherein the token set comprises at least two tokens, and wherein each token in the token set comprises at least two symbols that belong to the set of symbols;

requiring the user to select a token from the token set for each pin position in the passcode via the user interface; and

authenticating the user based on the tokens that the user selected, wherein the user is authenticated if:

the number of tokens selected by the user is equal to the number of symbols in the passcode,

at least one of the tokens selected contains a respective one of the passcode symbols, and

the pin position of each of the selected tokens that contains a respective one of the passcode symbols corresponds to the pin position of its respective passcode symbol in the passcode.

2. The method of claim 1, wherein the user is authenticated if:

the number of tokens selected by the user is equal to the number of symbols in the passcode;

each token selected contains a respective one of the passcode symbols; and

the pin position of each of the selected tokens corresponds to the pin position of each of the passcode symbols, based on which of the symbols in the passcode is included in each of the chosen tokens.

3. The method of claim 1, wherein the number of symbols in the set of symbols is equal to the number of tokens presented to the user.

4. The method of claim 1, wherein the number of symbols in the set of symbols is greater than the number of tokens presented to the user.

5. The method of claim 1, wherein each token comprises four symbols that belong to the set of symbols.
6. The method of claim 5, wherein each set of symbols is divided into four subsets ("dimensions") and each token comprises a symbol from each dimension of symbols.
7. The method of claim 1, wherein each token comprises five symbols that belong to the set of symbols.
8. The method of claim 7, wherein each set of symbols is divided into five subsets ("dimensions") and each token comprises a symbol from each dimension of symbols.
9. The method of claim 1, wherein the set of symbols is based on the Unicode system.
10. The method of claim 1, wherein the set of symbols is divided into at least two subsets ("dimensions") and each token comprises a symbol from each of the at least two dimensions.
11. A system for allowing a user access to electronically stored information ("authenticating") using a predetermined electronically stored passcode ("passcode") that comprises a predetermined number of symbols ("passcode symbols") selected from a set of symbols, wherein each of the passcode symbols is characterized by a predetermined pin position, comprising:
 - a processor;
 - memory accessible by the processor; and
 - an authentication/encryption module comprising a set of computer readable instructions stored in memory that are executable by the processor to:
 - present a token set to the user, wherein the token set comprises at least two tokens, and wherein each token in the token set comprises at least two symbols that belong to the set of symbols;
 - require the user to select a token from the token set for each pin position in the passcode via a user interface; and
 - authenticate the user based on the tokens that the user selected, wherein the processor determines that the user is authenticated if:

the number of tokens selected by the user is equal to the number of symbols in the passcode,

at least one of the tokens selected contains a respective one of the passcode symbols, and

the pin position of each of the selected tokens that contains a respective one of the passcode symbols corresponds to the pin position of its respective passcode symbol in the passcode.

12. The system of claim 11, wherein the processor determines that the user is authenticated if:

the number of tokens selected by the user is equal to the number of symbols in the passcode;

each token selected contains a respective one of the passcode symbols; and

the pin position of each of the selected tokens corresponds to the pin position of each of the passcode symbols, based on which of the symbols in the passcode is included in each of the chosen tokens.

13. The system of claim 11, wherein the number of symbols in the set of symbols is equal to the number of tokens presented to the user.

14. The system of claim 11, wherein the number of symbols in the set of symbols is greater than the number of tokens presented to the user.

15. The system of claim 11, wherein each token comprises four symbols that belong to the set of symbols.

16. The system of claim 15, wherein each set of symbols is divided into four subsets ("dimensions") and each token comprises a symbol from each dimension of symbols.

17. The system of claim 11, wherein each token comprises five symbols that belong to the set of symbols.

18. The system of claim 17, wherein each set of symbols is divided into five subsets ("dimensions") and each token comprises a symbol from each dimension of symbols.

19. The system of claim 11, wherein the set of symbols is based on the Unicode system.
20. The system of claim 11, wherein the set of symbols is divided into at least two subsets ("dimensions") and each token comprises a symbol from each of the at least two dimensions.