(19) **United States**

(12) **Patent Application Publication** (10) Pub. No.: **US 2010/0064360 A1**

Lin et al. (43) **Pub. Date: Mar. 11, 2010**

---

(54) **TOKEN DEVICE THAT GENERATES AND DISPLAYS ONE-TIME PASSWORDS AND THAT COUPLES TO A COMPUTER FOR INPUTTING OR RECEIVING DATA FOR GENERATING AND OUTPUTTING ONE-TIME PASSWORDS AND OTHER FUNCTIONS**

(75) Inventors: **Paul Lin**, Fremont, CA (US);
Henry Hon, Berkeley, CA (US)

Correspondence Address:
Stevens Law Group
1754 Technology Drive, Suite #226
San Jose, CA 95110 (US)

(73) Assignee: **Authenex, Inc.**, San Jose, CA (US)

(21) Appl. No.: **12/398,887**

(22) Filed: **Mar. 5, 2009**

Related U.S. Application Data

(63) Continuation of application No. 10/891,598, filed on Jul. 15, 2004, now Pat. No. 7,519,989.

(60) Provisional application No. 60/488,585, filed on Jul. 17, 2003.

Publication Classification

(51) **Int. Cl.**
G06F 7/04	(2006.01)
G06F 7/58	(2006.01)
H04L 9/00	(2006.01)
H04K 1/00	(2006.01)

(52) **U.S. Cl.** **726/9**; 726/20; 713/172

(57) **ABSTRACT**

A token device that generates and displays one-time passwords and couples to a computer for inputting or receiving data for generating and outputting one-time passwords and performing other functions is provided. The token includes an interface for coupling to a computer. The token may also be coupled to any network that the computer may be connected to, when coupled to the computer. Data and information may be transmitted between the computer and token, and between the network and token, via the computer and interface. The data and information may include one-time password seeding, file transfer, authentication, configuration and programming of the token. The token must be seeded to generate and display one-time passwords. An original, or seed, value is loaded into the token. One-time passwords are subsequently generated or calculated, or both, from the seed value. Seeding of the token involving a counter, time, or time-related functions, may allow synchronization of the token with such functions. The token may support different authentication methods.
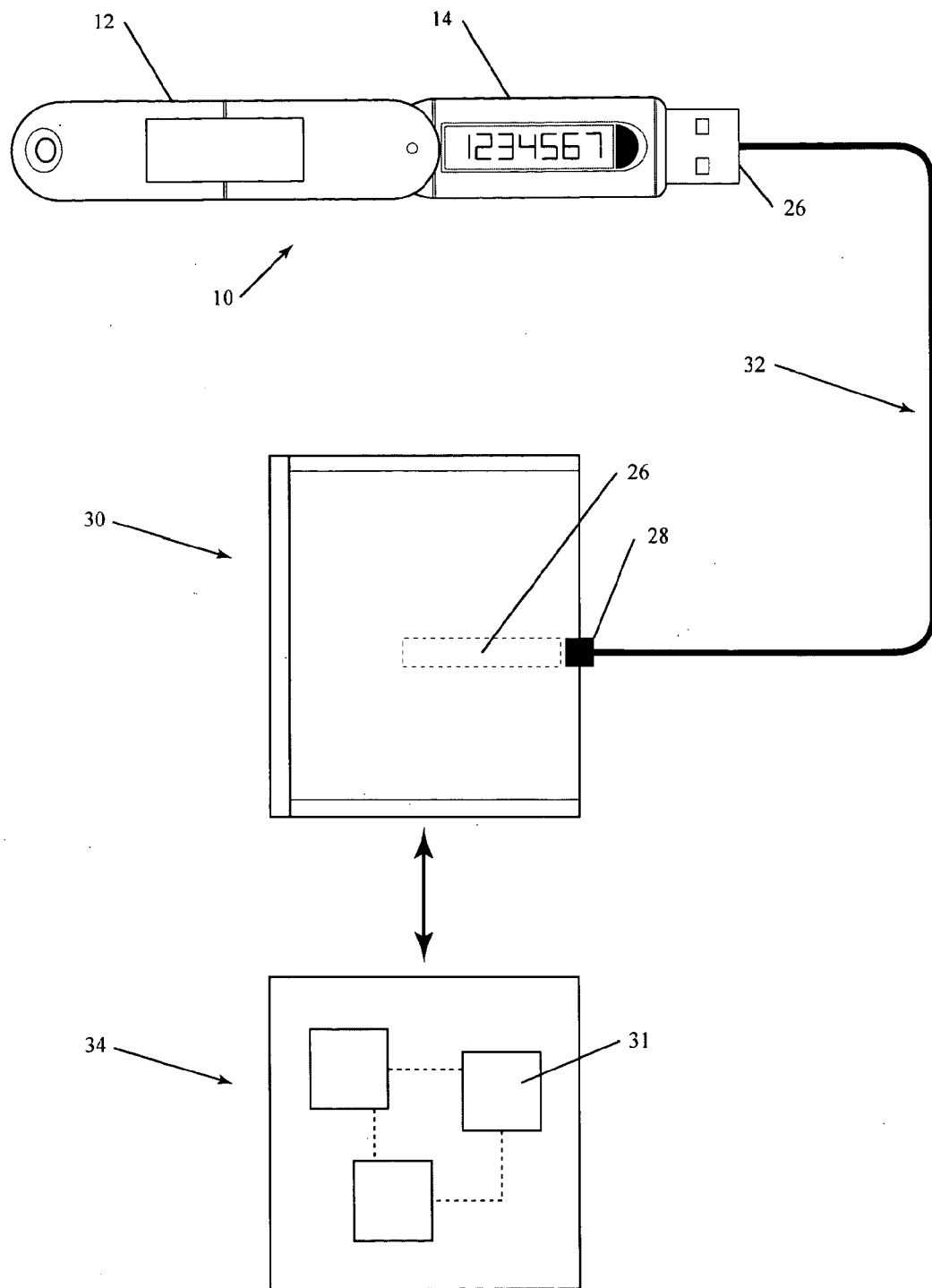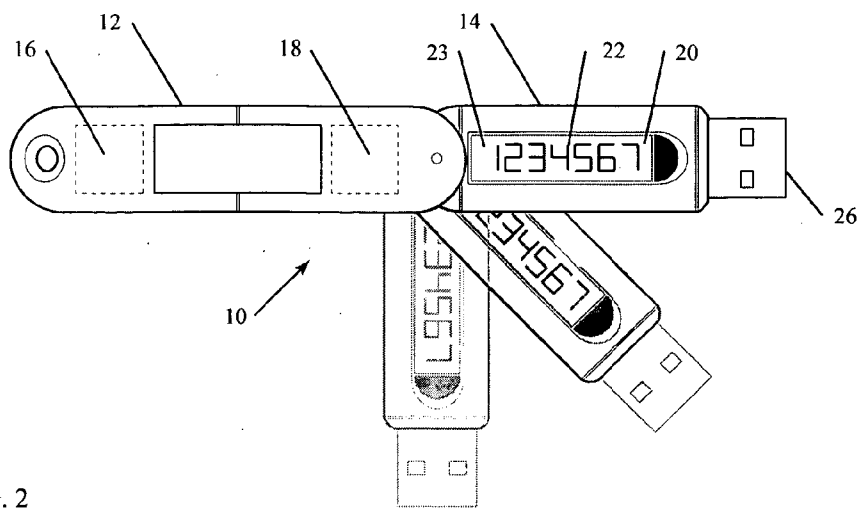
12

14

1234567
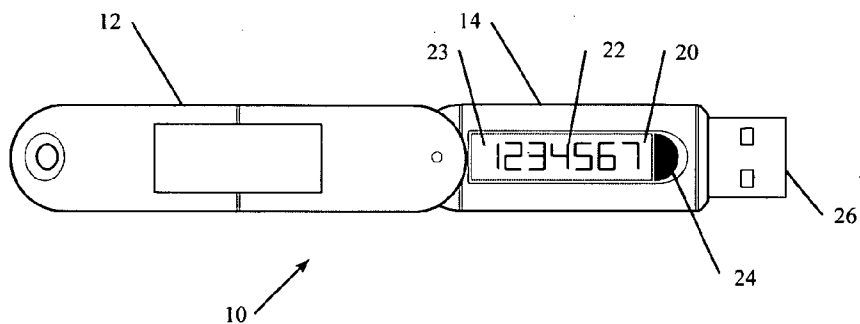
10

26

32

26

30

28

34

31
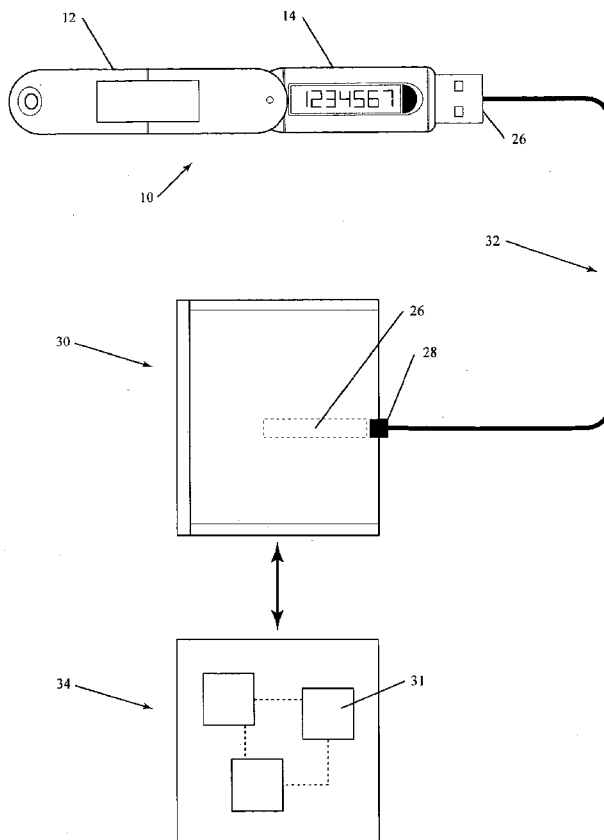
FIG. 1

FIG. 2

FIG. 3

FIG. 4

TOKEN DEVICE THAT GENERATES AND DISPLAYS ONE-TIME PASSWORDS AND THAT COUPLES TO A COMPUTER FOR INPUTTING OR RECEIVING DATA FOR GENERATING AND OUTPUTTING ONE-TIME PASSWORDS AND OTHER FUNCTIONS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application is a non-provisional application of Provisional Application No. 60/488,585, filed on Jul. 17, 2003.

BACKGROUND OF THE INVENTION

[0002] 1. Field of the Invention

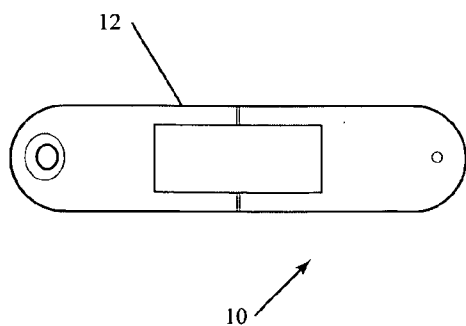[0003] The present invention relates to data authentication methods and systems and, more particularly, to a token device that generates and displays one-time passwords and couples to a computer for inputting or receiving data for generating and outputting one-time passwords and performing other functions.

[0004] 2. Background Information

[0005] The role of computers in our society has grown dramatically over the last few decades. During the past decade, networking technology and the Internet have grown and matured. The Internet is fast becoming the primary platform for global communication and commerce. However, the ease of communication and information sharing that has driven the growth of the Internet has also made it more difficult to ensure the security of Internet transactions and to maintain the privacy of information accessible over the Internet.

[0006] To maintain security and privacy, many transactions and communications taking place over the Internet and other networked environments require that a user authenticate him or herself in order to access information or to conduct transactions. For example, an online brokerage typically requires a user to authenticate him or herself prior to accessing their account or trading stocks.

[0007] Authentication refers to the method of proving the identity of the user. To be authenticated, the user typically presents a unique credential to a website or network they desire to access. This credential is usually comprised of a username and a secret password. Both the username and secret password may be established by the user. Alternatively, the username may be assigned to the user by an administrator of the website, or a similar entity, and the user may generate their secret password. Other known alternative methods may also be used to generate the username and password.

[0008] Static usernames and passwords are the most common method of authentication in the networked environment. However, static usernames and passwords are prone to several types of attacks and impersonations such as "Trojan horses" and "dictionary attacks." A user's static username and password can also be misappropriated through networking sniffers, password hacking programs, and other less sophisticated methods such as guesswork. For example, a user may have established a "weak" password using his date of birth or the name of his spouse as the password which may be easily guessed.

[0009] To strengthen authentication methods and prevent the types of attacks and impersonations described above, the network security industry has develop methods of authentication that go beyond simple username and password schemes. These methods may be categorized as challenge and response, Public Key Infrastructure or PKI, and One-Time-Password or OTP. These methods make impersonation attacks more difficult by creating longer and dynamic passwords. Longer passwords make it more difficult to guess the password, while dynamic passwords allow the authorized user to use the same username, but a new password each time.

[0010] Each new password is generated by hardware or software commonly referred to as a token device, or "token". The token may be designed to display dynamic passwords. When authentication is needed, the user simply enters the dynamic password displayed by the token at that time. These token values are often supplemented with a secret PIN code know only to the user. A secret PIN code may also be used to activate the token in order to display the dynamic password. These authentication methods have the potential to replace simple username and password schemes in the future.

BRIEF SUMMARY OF THE INVENTION

[0011] The present invention comprises a token device that generates and displays one-time passwords. The token device, hereinafter token, couples to a computer for inputting or receiving data for generating and outputting one-time passwords and performing other functions.

[0012] The token includes an interface for coupling to a computer. The token may be coupled to any network that the computer may be connected to. Data may be transmitted between the computer and token and between the network and token, via the computer and interface when the token is coupled to the computer and when the computer is connected to the network.

[0013] The data may include one-time password seeding, authentication, token configuration, programming of the token, and file transfer. The token may be multi-functional and capable of generating and displaying one-time passwords as well as performing other functions, such as challenge and response, PKI, digital certificate, and/or biometric.

[0014] The token must first be seeded to generate and display one-time passwords. Seeding is the process of loading an original, or seed, value into a token. From the seed value one-time passwords are subsequently generated or calculated, or both. There are many ways to load seed values into the token.

[0015] The token can be seeded when it is coupled to a computer via the interface. For example, seed values can be loaded into the token from the computer via the interface. Seed values may also be sent to the token from a network that the computer is connected to. The seed values may be encrypted or in clear text. The seed values may also be generated, derived and/or calculated from PKI keys pairs and/or digital certificates. Some methods of seeding involve a counter, time, or time-related functions. In these cases, when the token is coupled to a computer, it may allow synchronization operations to synchronize the token with such counter, time, or time related functions.

[0016] The token may support a single authentication method or a combination of different authentication methods. These authentication methods include one-time password, challenge response, PKI, digital certificate, and/or biometric.

The token may also perform such functions while coupled with a computer and thus to a network that the computer is connected to.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017] The objects and features of the present invention, which are believed to be novel, are set forth with particularity in the appended claims. The present invention, both as to its organization and manner of operation, together with further objects and advantages, may best be understood by reference to the following description, taken in connection with the accompanying drawings, in which:

[0018] FIG. 1 is a schematic diagram showing an embodiment of the token device of the present invention coupled to a computer and showing the computer coupled to a computer network;

[0019] FIG. 2 is a top, schematic view of a preferred embodiment of a token device of the invention showing a display portion rotatably coupled to a body portion of the token device invention;

[0020] FIG. 3 is a top, schematic view of a preferred embodiment of the token device of the invention; and

[0021] FIG. 4 is a top, schematic view showing token device of the invention in a closed position.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0022] The following description is provided to enable any person skilled in the art to make and use the invention and sets forth the best modes presently contemplated by the inventors of carrying out the invention. Various modifications, however, will remain readily apparent to those skilled in the art, since the generic principles of the present invention have been defined herein.

[0023] Referring to the drawing in FIGS. 1-4, the invention comprises a token device, or token, shown generally at 10. The token includes a body portion 12 and a display portion 14. The display portion may optionally be pivotally, rotatably, or similarly coupled to the body portion 12.

[0024] An on-board processor 16 and memory 18 for processing and storing data may be contained in the body portion 12. The processor 16 is preferably capable of generating and outputting data that may be utilized as one-time passwords. The one-time passwords output by the processor 16 may be displayed on a display 20 of the display portion 14.

[0025] A one-time password output by the processor 16 may comprise a string of alphanumeric characters. Preferably, the string of alphanumeric characters ranges from six to eight characters.

[0026] The token 10 may be provided with a unique string of information, or data, for identifying that particular token 10. The unique string of information may be stored in the token's memory 18. A copy of the unique string of information may reside at a remote location, such as a server 31 of a network 34.

[0027] The display portion 14 includes a display 20. The display 20 preferably comprises either a Liquid Crystal Display (LCD) or Light Emitting Diode (LED) display that is electronically coupled to the processor 16 using known methods. The display 20 is preferably capable of displaying a plurality of numeric or alphanumeric characters, shown generally at 22 that can be viewed through a window 23. The display portion 14 may be rotatably coupled to the body

portion 12. Rotatably coupling the display portion 14 to the body portion 12 may help to prevent damage to the display 20 and may provide a token 10 having reduced dimensions.

[0028] The display portion 14 includes an interface 26 for coupling the token 10 to a data port 28 of a computer, shown generally at 30. The interface 26 may be provided in any suitable known data interface configuration. Preferably, the interface 26 is provided in a known Universal Serial Bus (USB) configuration for coupling to a known USB port 28 of the computer 30 via a USB data cable 32. Additionally, the computer 30 may be coupled to a computer network 34, such as the Internet. Thus, data may be transmitted between the token 10 and computer 30, via the data cable 32, and data may be transmitted between the token 10 and network 34, via the data cable 32 and computer 30. Alternatively, the token 10 may optionally function externally of the network 34 and without coupling to the computer 30.

[0029] The display portion 14 may further include an activation button 24. The activation button 24 may be provided for activating the display 20, to limit power consumption or increase the life of the display 20, for example.

[0030] The token 10 is capable of receiving, generating, and outputting data and information. This data and information may include one-time password seeding, file transfer, authentication, configuration and programming of the token 10. The multi-functional token 10 is capable of generating and displaying one-time passwords as well as performing other functions.

[0031] The token 10 must first be seeded to generate and display one-time passwords. Seeding is the process of loading an original, or seed, data value into the token 10. From the seed value one-time passwords are subsequently generated or calculated, or both. There are many ways to load seed data values into the token 10.

[0032] One preferred method of seeding the token 10 includes first coupling the token 10 to the computer 30 via the data cable 32. The seed data values are then sent to the token 10 and stored in memory 18 and processed by the token's processor 16. Alternatively, seed values are then sent to the token 10 from a server 31 of the network 34 via the computer 30 and data cable 32. There are a number of known methods for transmitting and loading seed values into the token 10 that are readily apparent to those of ordinary skill in the art.

[0033] The seed data values may, or may not, be encrypted. The seed values may also be generated, derived and/or calculated from PKI keys pairs and/or digital certificates. Some methods of seeding the token 10 involve a counter, time, or time-related functions. In these cases, when the token 10 is coupled to the computer 30, it may allow synchronization operations to synchronize the token 10 with such counter, time or time related functions.

[0034] The token 10 may support a single authentication method or a combination of different authentication methods. These methods include one-time password, challenge response, PKI, digital certificate, and/or biometric. The token 10 may also perform such functions while coupled with the computer 30 and thus to any network 34 that the computer 30 is connected to.

[0035] Thus, there has been described a token device that generates and displays one-time passwords and couples to a computer for inputting or receiving data for generating and outputting one-time passwords and performing other functions. The token may also be coupled to any network that the computer may be connected to, when coupled to the com-

puter. Data and information may be transmitted between the computer and token, and between the network and token, via the computer and interface. The data and information may include one-time password seeding, file transfer, authentication, configuration and programming of the token.

[0036] Those skilled in the art will appreciate that various adaptations and modifications of the just-described preferred embodiments can be configured without departing from the scope and spirit of the invention. Therefore, it is to be understood that, within the scope of the appended claims, the invention may be practiced other than as specifically described herein.

What is claimed is:

1. A token device for generating and displaying password data comprising: a body portion; and a display portion, the display portion including a display for displaying alphanumeric characters and an interface for coupling the token to a computer.

2. The token device of claim 1 wherein the display portion displays alphanumeric characters representing password data generated by the token device.

3. A token device for generating and displaying password data comprising: a body portion, the body portion including, a processor for processing data; a memory for storing data, the memory coupled to the processor; and a display portion, the display portion including, a display for displaying alphanumeric characters, the display coupled to the processor for displaying data output by the processor; and an interface for coupling the token to a computer, for transmitting data between the processor and computer.

4. The token device of claim 3 wherein the display portion is rotatably coupled to the body portion.

5. The token device of claim 4 wherein the display displays alphanumeric characters representing password data output by the processor.

6. The token device of claim 5 wherein the display is configured to display at least five alphanumeric characters representing password data output by the processor.

7. The token device of claim 3 further including a data cable configured to couple the interface to the computer for transmitting data between the token device and computer.

8. A token device for generating and displaying password data comprising: a body portion, the body portion including, a processor for processing data, the processor contained within the body portion; a memory for storing data, the memory coupled to the processor and contained within the body portion; and a display portion rotatably coupled to the body portion, the display portion including, a display for displaying alphanumeric characters, the display coupled to the processor for displaying data output by the processor; and an interface for coupling the token to a computer, the interface coupled to the processor for transmitting data between the processor and computer.

9. The token device of claim 8 wherein the display is configured to display at least five alphanumeric characters representing password data output by the processor.

10. The token device of claim 9 wherein the display comprises a selected one of a liquid crystal display and a light emitting diode display.

11. The token device of claim 8 further including a data cable configured to couple the interface to the computer for transmitting data between the token device and computer.

12. The token device of claim 8 wherein the processor generates new password data at predetermined time intervals.

13. The token device of claim 8 wherein the processor generates new password data upon receipt of data from the computer, and wherein the new password data is displayed on the display.

14. The token device of claim 13 wherein the token device transmits the new password data to the computer via the data cable.

15. The token device of claim 14 wherein the computer is connected to a least one computer of a computer network.

16. The token device of claim 15 wherein the processor generates new password data upon receipt of data from a least one computer of the computer network that the token is connected to via the computer and data cable, and wherein the new password data is displayed on the display.

17. The token device of claim 16 wherein the token device transmits the new password data to least one computer of the computer network.

18. A method for generating and outputting one-time passwords, the method comprising; providing a token device, the token device including, a body portion including a processor and a memory; and a display portion, the display portion including a display for displaying alphanumeric characters representative of one-time password data generated by the processor, and an interface for coupling the token to a computer, for transmitting data between the token and computer; loading a value into the memory; feeding the value into the processor for generating data representative of one-time passwords; and generating data representative of a one-time password.

19. The method of claim 18 wherein the data representative of a one-time password is displayed on the display.

20. The method of claim 18 further comprising: providing a data cable configured to couple the interface to the computer for transmitting data between the token device and computer, and wherein the computer is connected to a least one computer of a computer network

21. The method of claim 20 further comprising: transmitting data representative of a one-time password from the token device to the computer.

22. The method of claim 21 further comprising: transmitting data representative of a one-time password from the token device to a computer of the computer network.

* * * * *